TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

JUHA JOKINEN

VERKKOLAITTEIDEN HALLINTA JA VALVONTA IPv6-VERKKO-YMPÄRISTÖSSÄ

Diplomityö

Tarkastaja: professori Jarmo Harju
Tarkastaja ja aihe hyväksytty
Tieto- ja sähkötekniikan tiedekuntaneuvoston kokouksessa 9. maaliskuuta 2016

TIIVISTELMÄ

JUHA JOKINEN: Verkkolaitteiden hallinta ja valvonta IPv6-verkkoympäristössä
Tampereen teknillinen yliopisto
Diplomityö, 71 sivua, 2 liitesivua
Syyskuu 2016
Tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Communication Systems and Networks
Tarkastaja: professori Jarmo Harju

Avainsanat: IPv6, verkkolaitteiden hallinta, Telnet, SSH, SNMP

Verkkolaitteiden hallinta ja valvonta ovat oleellinen osa organisaatioiden verkkojen toiminnan ylläpitämistä. Verkkolaitteiden valvonnan tehtävänä on välittää hallintatietoa verkosta ja verkossa sijaitsevista verkkolaitteista verkon ylläpidosta vastuussa oleville henkilöille. Hallinnan ja erityisesti verkkolaitteisiin muodostettavien etäyhteyksien tarkoituksena on mahdollistaa nopea reagointi verkossa tapahtuviin poikkeamatilanteisiin ja mahdollistaa etäyhteyksin verkkolaitteiden konfiguraatioiden muuttaminen.

Tämän työn tavoitteena on selvittää, kuinka verkkolaitteiden hallinta ja valvonta voidaan toteuttaa IPv6-osoitteisessa verkkoympäristössä. Työ perustuu aiheen teoreettiseen tarkasteluun kirjallisuustutkimusten avulla sekä käytännön tutkimuksiin työtä varten erikseen rakennetussa laboratorioympäristössä. Laboratorioympäristössä suoritettavien tutkimusten tavoitteena on selvittää käytännön menetelmin kahden verkkolaitteiden etähallintaan käytettävän protokollan Telnetin ja SSH:n toimivuus yhdessä IPv6-protokollan kanssa. Lisäksi tutkimuksissa on tarkoitus selvittää erityisesti verkonvalvontaan tarkoitetun SNMP-protokollan toimivuus IPv6-osoitteisessa ympäristössä sekä tutkia, kuinka verkossa sijaitseville kytkimille voidaan luoda IPv6-protokollalla toteutettuja etäyhteyksiä sallivia ja estäviä pääsylistoja ja kuinka ne toimivat.

Tutkimuksia varten rakennettu laboratorioympäristö koostuu useista eri laitevalmistajien erimallisista verkkolaitteista, joiden toimivuutta eri hallinta- ja valvontaprotokollien kanssa on tarkoitus tutkia, kun verkkolaitteiden hallintaosoitteistus on toteutettu IPv6-protokollalla. Tutkimuksista saatujen tulosten perusteella tehdään päätelmiä siitä, voitaisiinko tutkittavien verkkolaitteiden osalta toteuttaa vastaavanlainen verkkolaitteiden hallinta ja valvonta IPv6-protokollalla kuin se on nyt toteutettu vanhemmalla IPv4-protokollalla. Lisäksi tavoitteena on saada selville niitä laite- ja protokollakohtaisia rajoitteita, joilla voisi olla vaikutusta hallinta- ja valvontayhteyksien toteuttamiseen IPv6-protokollalla.

Tutkimustulokset osoittivat, että kaikki IPv6-protokollaa tukevat verkkolaitteet toimivat ongelmitta tutkittavien protokollien kanssa. Lisäksi kytkimiin luoduilla pääsylistoilla onnistuttiin sekä estämään että sallimaan tietystä IPv6-lähdeosoitteesta saapuvat etäyhteydet. Yleisesti tutkimustuloksista voidaan sanoa, että verkkolaitteiden näkökulmasta laitteiden hallinta ja valvonta voitaisiin toteuttaa myös IPv6-osoitteisessa verkkoympäristössä. Eri laitevalmistajien uusimmat laitemallit sekä niiden uusimmat ohjelmistoversiot ovat IPv6-protokollaa tukevia, joten laitteiden osalta ei ole minkäänlaisia rajoittavia tekijöitä hallinta- ja valvontayhteyksien muodostamisessa verkkolaitteisiin.

ABSTRACT

JUHA JOKINEN: Network device management and monitoring in IPv6 environment
Tampere University of Technology
Master of Science Thesis, 71 pages, 2 Appendix pages
September 2016
Master's Degree Programme in Information Technology
Major: Communication Systems and Networks
Examiner: Professor Jarmo Harju

Keywords: IPv6, network device management, Telnet, SSH, SNMP

Network device management and monitoring are an essential part of maintaining computer networks of organizations. The purpose of the network device monitoring is to provide management information for network administrators of networks and network devices residing in organization's local area networks. The purpose of the network device management and remote accesses are to make possible rapid response to the problems in the networks and to make possible the changing of device configurations via remote access.

The objective of this thesis is to research, how network device management and monitoring can be implemented in an IPv6 environment. The thesis is based on literature studies and practical experiments which are performed in a specific network laboratory which was built for this thesis. The goal of the laboratory experiments is to analyse, how Telnet and SSH protocols work together with the IPv6 protocol. Furthermore, it is intended to analyse, how the network monitoring protocol SNMP works in the IPv6 environment and how access lists work in the network switches when they are configured with IPv6 protocol.

The goal of the experiments is to find out, how different network device management and monitoring protocols work with different device models from different vendors, while the management interfaces in the network laboratory devices are configured with IPv6 protocol. The results are used to make conclusions of the fact whether the similar network device management and monitoring like it has been now carried out with IPv4 protocol could be formed for laboratory network devices with IPv6 protocol. In addition, the objective is to find out any protocol and device specific limitations that could affect creating management and monitoring connections to the devices with IPv6 protocol.

The research results showed, that all the network devices which support the IPv6 protocol worked without problems with all management and monitoring protocols in the IPv6 environment. Also we succeeded to configure access lists which blocked and permitted remote accesses from a certain IPv6 source address. On the basis of the research results we can say that network device management and monitoring could be implemented with IPv6 protocol from the network device point of view. All the newest device models and their software versions support the IPv6 protocol so there should not be any limitations implementing management connections in these devices in the IPv6 environment.

ALKUSANAT

Tämä diplomityö on tehty yhteistyössä TeliaSonera Finland Oyj:n ja erityisesti sen Customer Network Services 2 -verkonhallintatiimin kanssa. Tämän kahdeksan kuukauden urakan aikana olen oppinut työni tutkimusaiheesta paljon ja toivottavasti tästä on minulle hyötyä tulevaisuudessa.

Haluan kiittää diplomityöni tarkastajaa professori Jarmo Harjua, joka on asiantuntevasti kommentoinut työtäni matkan varrella ja ohjannut minua saavuttamaan päämääräni. Suuri kiitos kuuluu työpaikalleni TeliaSonera Finland Oyj:lle, joka mahdollisti tämän työn tekemisen. Erityisesti haluan kiittää kollegoitani niin työn aiheen ideoinnista kuin myös avustuksesta tutkimusten teossa.

Lopuksi haluan kiittää kaikki niitä läheisiä ihmisiä, jotka ovat kannustaneet minua tämän pitkän, mutta opettavaisen matkan aikana, kiitos.

Tampereella, 23.8.2016

Juha Jokinen

SISÄLLYSLUETTELO

LIITE A: Laboratorioverkon laitteiden pääsylistatutkimuksiin liittyvät konfiguraatiot

KÄSITTEET JA LYHENTEET

AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
EUI-64	Extended Unique Identifier
Fa	Fast Ethernet
Ge	Gigabit Ethernet
Gi	Gigabit Ethernet
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv4	Internet Control Message Protocol version 4
ICMPv6	Internet Control Message Protocol version 6
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Membership Protocol
HP	Hewlett-Packard
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 4
ISO	International Organization for Standardization
MAC	Media Access Control
MIB	Management Information Base

MTU	Maximum Transmission Unit
NA	Neighbor Advertisement
NAT	Network Address Translation
NDP	Neighbor Discovery Protocol
NS	Neighbor Solicitation
NVT	Network Virtual Terminal
OID	Object Identifier
OUI	Organizationally Unique Identifier
PIM	Physical Interface Module
PMTUD	Path Maximum Transmission Unit Discovery
RA	Router Advertisement
RARP	Reverse Address Resolution Protocol
RFC	Request for Comments
RIR	Regional Internet Registry
RS	Router Solicitation
RSA	Rivest, Shamir, Adleman
SDM	Switch Database Management
SNMP	Simple Network Management Protocol
SNMPv1	Simple Network Management Protocol version 1
SNMPv2	Simple Network Management Protocol version 2
SNMPv3	Simple Network Management Protocol version 3
SSH	Secure Shell
SSH-1	SSH version 1
SSH-2	SSH version 2
SSH-AUTH	Secure Shell Authentication Protocol

SSH-TRANS	Secure Shell Transport Layer Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
Te	TenGigabit Ethernet
TTL	Time To Live
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WAN	Wide Area Network

1. JOHDANTO

Johdantoluvussa käsitellään ensin työn taustatekijöitä, jonka jälkeen määritellään työn tavoitteet, tutkimusongelmat sekä rajataan aihe työssä tehtävien tutkimusten ja tutkimusalueen osalta. Lopuksi esitellään työn sisältöä selvittäen, mistä osista työ koostuu ja miten työn rakenne on muodostettu.

1.1 Taustaa

Tieto IPv4-osoitteiden loppumisesta on alun perin johtanut uudemman IPv6-protokollan kehittämiseen ja vähitellen myös sen laajempaan käyttöönottoon. Kun IANA (Internet Assigned Numbers Authority) ilmoitti helmikuussa 2011 jaettavien IPv4-osoitteiden olevan käytännössä loppu, oli jo selvää, että IPv6-protokolla on tulevaisuudessa todennäköisin vaihtoehto korvaamaan vanhemman IPv4-protokollan ja siten IPv4-osoitteistuksen verkossa (Cui et. al. 2015). Vaikka IPv6-protokolla ja siten IPv6-osoitteet ovat olleet käytössä jo pidemmän aikaa, on protokollan käyttöönotto ollut verrattain hidasta johtuen lukuisista yksittäistä asioista. Osaltaan protokollan hidas käyttöönotto johtunee siitä, että IPv4-protokolla on tarjonnut toimivan verkkoprotokollan aina tähän päivään saakka siitä lähtien, kun IPv4-standardi määriteltiin vuonna 1981. Tästä syystä useat verkon laitteet ovat edelleen ainoastaan IPv4-protokollaa tukevia, joten IPv6-protokollan kokonaisvaltainen käyttöönotto vaatisi suuria rahallisia panostuksia, koska verkossa olevia verkkolaitteita kuten reitittimiä ja kytkimiä jouduttaisiin korvaamaan uudemmilla myös IPv6-protokollaa tukevilla vaihtoehdoilla. IP-protokollaversiot eivät myöskään ole keskenään suoraan yhteentoimivia, vaan niiden välille tarvitaan erityisiä verkkoteknisiä ratkaisuja, jotta ne saadaan toimimaan keskenään, mikä on entisestään hidastanut IPv6:n yleistymistä kolmannen tason verkkoprotokollana. Lisäksi IPv4-osoitteiden loppumisen haittavaikutuksia on pystytty minimoimaan erilaisilla verkkoteknisillä ratkaisuilla kuten esimerkiksi NAT-tekniikoilla (Network Address Translation) (Levin & Schmidt 2014). Niin kauan kuin vaihtoehtoisilla verkkoratkaisuilla voidaan jatkaa IPv4-protokollan elinkaarta, ei IPv6-protokollaan siirtymiseen ole pakottavia tekijöitä. Uuden IP-protokollan uskotaan kuitenkin olevan ainoa kestävä pitkäaikaisratkaisu IPv4-osoitteiden loppumiselle (Levin & Schmidt 2014).

Siirtyminen IPv6-protokollalla toteutettuihin verkkoihin on yhä yksi tärkeimmistä IETF:n (Internet Engineering Task Force) käsittelemistä aiheista (Cui et. al 2015). IPv6-protokollan käyttöönotto on vaatinut paljon tutkimustyötä ja vaatii sitä edelleen, jotta voidaan varmistua kaikkien verkoissa sijaitsevien laitteiden ja järjestelmien toimivuudesta yhdessä tämän protokollan kanssa. Käyttöönotto on vaiheittainen prosessi, joka vaatii

tarkkaa suunnittelua ja ympäristöjen testaamista, jotta verkot saadaan toimimaan uuden protokollan kanssa samalla tavalla kuin ne tällä hetkellä toimivat vielä laajasti käytössä olevan IPv4-protokollan kanssa. Tällä hetkellä ollaan vahvasti siirtymävaiheessa, jossa molempia protokollia käytetään rinnakkain IPv4-protokollan ollessa edelleen laajemmin käytössä.

Organisaatioiden lähiverkot muodostuvat nykyään lukuisista aktiivisista verkkolaitteista kuten reitittimistä ja kytkimistä, joiden tarkoituksena on mahdollistaa organisaatioiden lähiverkkojen toiminta. Organisaatioiden verkkoyhteydet ovat riippuvaisia näiden verkkolaitteiden toiminnasta, joten on tärkeää, että verkkolaitteet toimivat oikein ja niille suunnitellulla tavalla. Usein organisaatiot ovat siirtäneet näiden laitteiden toiminnan varmistamisen verkko-operaattoreille tai muille verkkopalveluja tarjoaville organisaatioille, joiden tehtävä on varmistaa etähallinnan keinoin näiden verkon komponenttien toiminta. Verkkolaitteiden etähallinta ja -valvonta perustuvat verkkolaitteille asetettuihin IP-protokollan mukaisiin hallintaosoitteisiin. Nykyään vielä suuri osa verkkolaitteiden hallintayhteyksistä on toteutettu vanhemmalla IPv4-protokollalla, mutta IPv6-protokollan koko ajan laajeneva käyttöönotto tulee mitä luultavammin vaikuttamaan tulevaisuudessa myös laitteiden hallintayhteyksiä toteuttamiseen. Tästä syystä on tärkeä selvittää, kuinka nykyisten verkkolaitteiden hallinta- ja valvontayhteydet voidaan toteuttaa uudemmalla IP-protokollalla. Hallintayhteyksien toiminnan varmistamiseksi on tärkeä selvittää, miten eri valmistajien verkkolaitteet toimivat yhdessä tämän protokollan kanssa ja, onko eri laitemallien välillä toteutusteknisiä asioita, jotka voisivat estää yhteyksien muodostamisen laitteisiin. Jotta voidaan varmistua hallintayhteyksien toimivuudesta eri verkkolaitteisiin, tulee yhteyksien toimivuutta testata IPv6-protokollalla toteutetussa ympäristössä, joka mallintaa mahdollisimman tarkasti todellisia verkkoympäristöjä.

1.2 Tavoitteet, tutkimusongelmat ja tutkimuksen rajaus

Tämän työn tavoitteena on tutkia, kuinka verkkolaitteiden hallinta ja valvonta voidaan toteuttaa IPv6-osoitteisessa verkkoympäristössä. Tarkoituksena on tutkia eri verkkolaitteiden etähallintaan ja -valvontaan liittyvien protokollien toimivuutta IPv6-osoitteisessa ympäristössä ja tehdä päätelmiä, voidaanko vastaavanlaista verkonhallintaa toteuttaa IPv6-protokollan avulla kuin se tällä hetkellä on toteutettu vanhemman IPv4-protokollan avulla. Työn päätutkimusongelmana on selvittää:

- ***Kuinka verkkolaitteiden hallinta- ja valvontayhteydet voidaan toteuttaa IPv6-protokollalla toteutetussa verkkoympäristössä?***

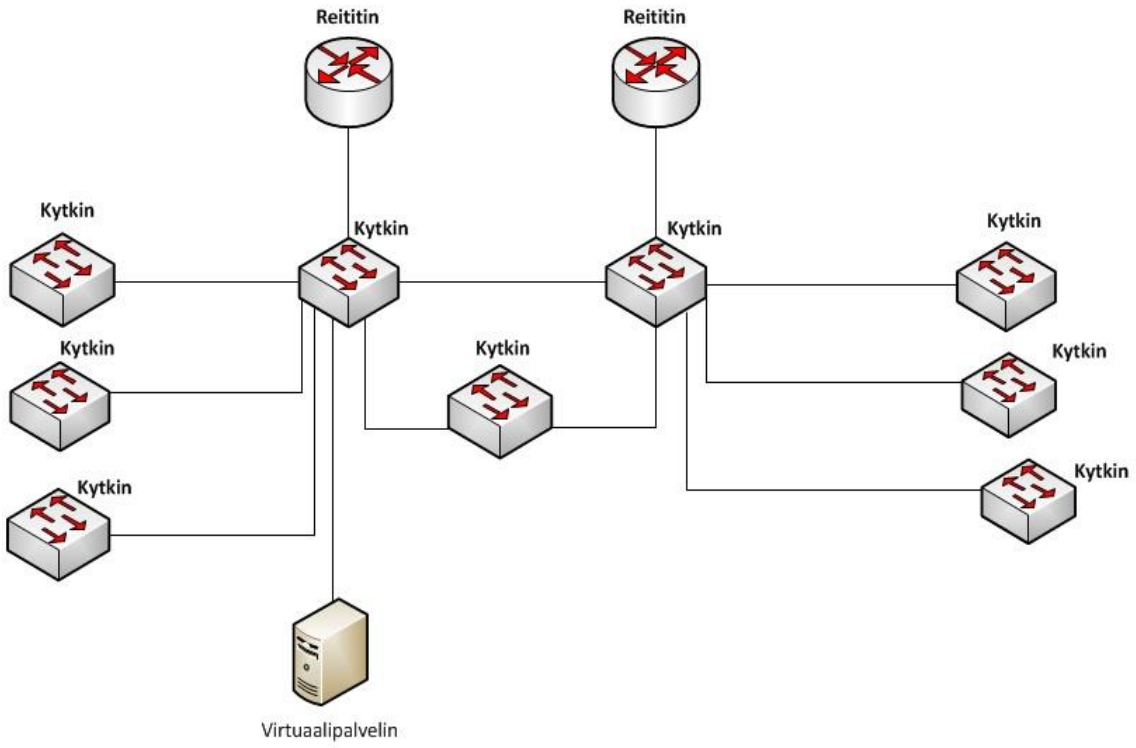
Päätutkimusongelman toteutumista tutkitaan etsimällä vastauksia seuraavassa esitettyihin tutkimuskysymyksiin:

- Minkälaisia konfiguraatioita verkkolaitteet vaativat, jotta IPv6-protokolla saadaan otettua käyttöön tutkittavissa laitteissa?

- Kuinka verkkolaitteiden hallintaosoitteistus voidaan toteuttaa IPv6-protokollalla?
- Voidaanko Telnet-, SSH- (Secure Shell) ja SNMP-protokollia (Simple Network Management Protocol) käyttää IPv6-osoitteisessa verkkoympäristössä?
- Kuinka kytkimille voidaan luoda etäyhteyksiä sallivia tai estäviä IPv6-pääsylistoja? Toimivatko muodostetut pääsylistat samalla tavalla IPv6-protokollan kanssa kuin IPv4-protokollan kanssa?
- Onko eri laitevalmistajien laitteiden ja vastaavasti laitemallien välillä erovaisuuksia hallinta- ja valvontayhteyksien toteuttamisessa?

Työssä pyritään etsimään vastauksia edellä esitettyihin kysymyksiin, joiden avulla pyritään vastaamaan työn päätutkimusongelmaan. Tutkimuskysymysten tarkoituksena on jakaa päätutkimusongelma pienempiin osiin, joiden pohjalta voidaan tehdä päätelmiä siitä, kuinka päätutkimusongelma toteutuu.

Työn tutkimusosa suoritetaan kuvan 1.1 mukaisessa laboratorioympäristössä, jossa tehtävien tutkimusten avulla pyritään löytämään vastauksia edellä määritettyihin tutkimuskysymyksiin.



Kuva 1.1. *Työn tutkimusalueen rajaus.*

Kuvassa on esitetty työn tutkimusten tarkastelualue, joka koostuu ennalta valitusta laitteistosta. Valittu laitteisto koostuu tämän työn yhteistyöorganisaation asiakkailleen eniten toimittamista laitteista, joten tutkimuksissa ei yleisesti oteta kantaa protokollan toimivuuteen kuin tiettyjen laitevalmistajien tietyn mallisissa laitteissa. Lisäksi tutkimuksissa kes-

kitytään lähiverkon toimintaan, eikä siinä siten oteta kantaa laajempien verkkokokonaisuuksien ja -teknisten asioiden toimintaan. Tutkimuksen kohteiksi valitut verkkolaitteiden hallinta- ja valvontaprotokollat ovat yleisimpiä etähallintaan ja -valvontaan käytettäviä protokollia, joita tämän työn yhteistyöorganisaatiossa käytetään päivittäin verkkolaitteiden hallintaan ja valvontaan liittyvissä prosesseissa.

1.3 Työn sisältö

Työ perustuu kirjallisuustutkimuksiin ja työn loppupuolelle suoritettaviin laboratoriotutkimuksiin. Työn sisältö koostuu johdanto- ja yhteenvetoluvun lisäksi kolmesta osasta: aiheen teoreettisesta tarkastelusta, tutkimusympäristön kuvauksesta sekä tutkimuksen läpikäynnistä ja tulosten tarkastelusta. Luvut kaksi ja kolme käsittelevät työn aihepiiriä teoreettisella tasolla ja niiden tavoitteena on tuoda esille niitä teoreettisia seikkoja, jotka ovat tärkeitä työn tavoitteiden ja laajemman ymmärtämisen kannalta. Luvuissa viitataan aiheesta tehtyihin aikaisempiin tutkimuksiin, joiden on tarkoitus toimia teoreettisina taustatietoina tässä työssä tehtäville tutkimuksille. Toisessa luvussa käsitellään verkkolaitteiden hallintaa ja valvontaa yleisellä tasolla. Selvitetään lukijalle, mitä hallinta- ja valvontakäsitteillä verkkolaitteiden kohdalla tarkoitetaan ja, miten ne näkyvät käytännön työssä. Lisäksi luvussa käsitellään verkkolaitteiden hallintaan ja valvontaan yleisesti käytettäviä teknisiä työkaluja teoreettisella tasolla.

Luvussa kolme käsitellään IPv6-protokollaa ensin yleisellä tasolla ottaen huomioon muutokset edelliseen IPv4-protokollaan verrattuna. Lisäksi protokollan teknistä toteutusta pyritään käsittelemään verkkolaitteiden hallinnan ja valvonnan näkökulmasta tuoden esille niitä teknisiä ominaisuuksia, joilla on merkitystä tämän näkökulman kannalta. Kolmannessa luvussa viitataan myös muihin IPv6-protokollan kehityksen yhteydessä toteutettuihin protokolliin, joilla on merkittävä rooli protokollan toiminnassa. Luvut kaksi ja kolme yhdessä muodostavat työn teoreettisimman osan ja ne perustuvat pääosin aihepiirin käsittelyyn kirjallisuustutkimusten avulla.

Neljännessä luvussa esitellään työssä tehtäviä tutkimuksia varten rakennettu laboratorioympäristö. Luvun tavoitteena selventää lukijalle laboratorioympäristön merkitys osana työssä tehtäviä tutkimuksia. Laboratorioympäristön kuvaaminen on olennaista tutkimusten suorittamisen seuraamisen kannalta. Neljännen luvun aiheen käsittely perustuu niin kirjallisuustutkimuksiin kuin omakohtaiseen tutkimustyöhön, joka on suoritettu käyttäen apuna aiheeseen liittyviä aikaisempia tutkimuksia. Neljäs luku toimii esitietona seuraavassa luvussa tehtäville tutkimuksille.

Viides luku muodostaa yhdessä edellisen luvun kanssa työn tutkimusosuuden. Luvussa tuodaan esille työssä tehtävien tutkimusten tavoitteet ja sen, kuinka tutkimukset on suunniteltu toteutettavaksi. Lisäksi siinä kuvataan yksityiskohtaisesti, kuinka työn alussa määritettyjen tutkimusongelmien toteutumisen tutkiminen laboratorioympäristössä suorite-

taan. Tutkimuksen läpikäynti pohjautuu yksityiskohtaiseen testaustilanteiden suorittamiseen havainnollistavien kuvien avulla. Lopuksi luvussa tuodaan esille tutkimuksissa aikaansaadut tulokset eritellen eri tutkimuskohteet ja eri verkkolaitteille kohdistetut tutkimukset. Tutkimuksissa saatujen tulosten perusteella tehdään päätelmiä siitä, kuinka tässä luvussa esiteltyihin tutkimuskysymyksiin ja siten päätutkimusongelmaan on löydetty vastauksia.

2. VERKKOLAITTEIDEN HALLINTA JA VALVONTA VERKOSSA

Verkkolaitteiden hallinnalla ja valvonnalla on merkittävä rooli organisaatioiden lähiverkkojen toiminnan kannalta, koska verkot ja niihin liittyvät resurssit ovat nykyään korvaamattomia organisaatioille. Kun verkkoon liitettävien laitteiden lukumäärä kasvaa, kasvaa samalla lähiverkkojen koko suuremmaksi sisältäen yhä enemmän verkkolaitteita, joiden toiminta on tärkeää verkkoyhteyksien kannalta ja siten usein edellytyksenä organisaatioiden liiketoiminnan jatkuvalle harjoittamiselle. (Stallings 1999) On siis tärkeää, että verkon tilaa voidaan valvoa ja mahdollisten ongelmatilanteiden sattuessa voidaan näihin tilanteisiin reagoida nopeasti etähallinnan avulla. Tässä luvussa esitellään lähiverkkojen hallinta ja valvonta käsitteinä sekä käsitellään yleisesti hallinnan ja valvonnan roolia verkkojen ylläpidon näkökulmasta. Lisäksi esitellään yleisimpiä laajasti käytössä olevia verkkolaitteiden hallinta- ja valvontaprotokollia, joiden soveltuvuutta IPv6-lähiverkkoympäristöön tutkitaan myöhemmin tässä työssä. Lopuksi luvussa määritellään vielä, mitä tässä työssä tarkoitetaan hallintaosoitetermillä.

2.1 Verkkolaitteiden hallinta ja valvonta yleisesti

Verkkolaitteiden lukumäärän kasvun seurauksena organisaatioiden lähiverkoissa on entistä enemmän komponentteja, jotka voivat syystä tai toisesta vikaantua aiheuttaen katkoksia verkkoyhteyksiin. Jotta verkkoympäristöt voivat toimia oikein ja ilman pitkiä yhteyskatkoksia, tarvitaan mahdollisuus tehdä nopeita hallintatoimenpiteitä sekä jatkuvaa automatisoitua verkonvalvontaa. Verkkolaitteiden konfiguraatiot on suunniteltu ja toteutettu siten, että niiden avulla verkko saadaan toimimaan siten kuin palvelun tilaaja on sen halunnut. Usein verkkolaitteiden konfiguraatiot ovat pitkäikäisiä eivätkä välttämättä vaadi juurikaan muutoksia ennen kuin laite korvataan uudella. Toisinaan verkkojen rakennetta tai toimintaa voidaan haluta muuttaa syystä tai toisesta, jolloin on tarve tehdä muutoksia myös verkkolaitteiden konfiguraatioihin. Toisinaan taas voi olla tarve tehdä nopeita muutoksia esimerkiksi viankorjauksen yhteydessä, jolloin on tärkeää, että laitteiden konfiguraatioita voidaan muuttaa välittömästi, jotta verkko saadaan takaisin toimintakuntoon mahdollisimman nopeasti. Tätä tarkoitusta varten on olennaista, että esimerkiksi palveluntarjoaja voi hallita asiakkaidensa verkkolaitteita keskitetysti etäyhteyksien avulla. Tässä etähallinnalla tarkoitetaan sitä, että verkonhallinnasta vastuussa olevat henkilöt voivat kirjautua etäältä verkkolaitteisiin ja näin tarkastella tai muuttaa niiden konfiguraatioita. Tällöin esimerkiksi verkkolaitteiden konfiguraatioiden muuttamisesta ei aiheudu ylimääräistä viivettä, vaan verkko on toimintakunnossa nopeammin kuin vastaava työ tehtäisiin paikallisesti laitteiden luona. Verkkolaitteiden hallintaan on tärkeä valita

oikeat protokollat, jotta verkkojen muuttuvaa luonnetta voidaan hallinnoida tehokkaasti. (Stallings 1999; Zheng & Cui 2010)

Verkonhallinta on kattokäsitteenä varsin laaja ja sen voidaan siten katsoa käsittävän lähes kaiken toiminnan verkkojen ylläpitämiseksi. Sillä voidaan viitata kaikkiin niihin toimintoihin, menetelmiin ja työkaluihin, jotka kuuluvat verkkojen ylläpitoon ja hallintaan. Toisin sanoen siihen liittyy vahvasti kaikki verkon ylläpitotoimet, viankorjaus, verkon resurssien valvonta ja verkkolaitteiden konfiguraatioiden muuttaminen tarpeiden muuttuessa. (Teltumde et al. 2012) Stallings esittelee teoksessaan (1999) ISO-standardointityöryhmän (International Organization for Standardization) luoman määritelmän verkonhallinnalle. Tämä verkonhallinnan viitekehys sisältää viisi toiminnallista aluetta, jotka verkonhallinnassa ja sen toteuttamisessa tulisi ottaa huomioon. ISO:n luomaa viitekehystä voidaan pitää laajempana määritelmänä verkonhallinnalle, jonka avulla verkonhallinnan kokonaisuus voidaan helpommin ymmärtää. Viitekehyksen viittä toiminnallista aluetta voidaan pitää myös vaatimuksina, joiden avulla verkonhallinnan toteutumista voidaan arvioida. Nämä viisi toiminnallista aluetta ovat:

- ***Vianhallinta***. Jotta verkko voi toimia oikein, tulee verkon kokonaisuudessaan ja tärkeiden laitteiden itsessään olla toimintakunnossa. Verkon ylläpitäjien täytyy pystyä havaitsemaan poikkeamatilanteet verkon toiminnassa, eristämään ne ja korjaamaan nämä poikkeamatilanteet. Olennaisena osana vianhallintaa on verkon valvonta, jotta vikojen lähde saadaan selvitettyä ja viat itsessään saadaan korjattua mahdollisimman nopeasti.
- ***Käytön hallinta***. Verkon ylläpitäjien tulee pystyä keräämään tietoa verkon käytöstä. Tätä tietoa voidaan edelleen käyttää esimerkiksi laskutukseen tai valvomaan verkon resurssien käyttöä. Verkon resurssien käytöstä saatua todellista tietoa voidaan käyttää esimerkiksi verkon tehokkuuden parantamiseen.
- ***Konfiguraation hallinta***. Verkot koostuvat laitteista ja järjestelmistä, joilla jokaisella on oma roolinsa verkon toiminnan kannalta. Konfiguraation hallinnan tehtävänä on alustaa verkko, ylläpitää ja muuttaa verkon laitteiden välisiä riippuvuuksia tarpeen mukaan. Verkkolaitteiden konfiguraatioita voi olla tarpeen muuttaa, kun havaitaan tarve muuttaa esimerkiksi verkon rakennetta.
- ***Suorituskyvyn hallinta***. Verkot koostuvat useista komponenteista, jotka jakavat resursseja keskenään. Verkon suorituskykyä tulee analysoida ja mitata, jotta verkon toiminta voidaan pitää hyväksyttävällä tasolla. Verkon suosituskyvyn hallinnan pääasiallisena tavoitteena on ylläpitää verkon suorituskyky optimaalisena.
- ***Turvallisuuden hallinta***. Pääsyä verkkoon ja verkossa oleviin laitteisiin valvotaan ja hallitaan. Ainoastaan valtuutetuilla henkilöillä tulee olla pääsy verkkolaitteisiin ja organisaation resursseihin. Erilaisten lokitietojen avulla voidaan valvoa pääsyä näihin resursseihin. Turvallisuuden hallinta on pääasiassa lokitietojen keräämistä, tallentamista ja tutkimista. (Stallings 1999; Shaffi & Al-Obaidy 2013)

Verkonhallintaan ja siten verkkolaitteiden hallintaan liittyy oleellisesti myös verkkolaitteiden valvonta, jonka pääasiallisena tehtävänä on valvoa verkkolaitteiden toimintaa ja havaita verkon mahdollisia poikkeamatilanteita. Verkonvalvonnan työkalujen tarkoituksena on tukea ja tehostaa verkkolaitteidenhallintaa mahdollistaen täysin automatisoitu verkonvalvonta, joka ei olisi mahdollista ihmisten suorittamana. Verkonvalvontajärjestelmillä voidaan tukea kaikkia viittä ISO-standardointityöryhmän verkonhallintamallissa esiintyvää toiminnallista aluetta (Shaffi & Al-Obaidy 2013). Verkon valvonnan ensisijainen tehtävä on siis auttaa verkonhallinnasta vastuussa olevia henkilöitä havaitsemaan verkon poikkeamatilanteet, jotta niistä voidaan toipua ilman suurempia viiveitä. Kun verkossa tai verkkolaitteessa ilmenee jokin poikkeamatilanne, esimerkiksi verkkolaitteiden välinen fyysinen linkki menee alas, täytyy verkkolaitteita valvovan järjestelmän pystyä antamaan ilmoitus syntyneestä poikkeamatilanteesta. Näin saavutetaan se, että verkon toiminnasta vastuussa olevat henkilöt saadaan tietoisiksi verkossa olevasta poikkeamatilanteesta ja mahdollisesti verkon osittaisesta tai täydellisestä toimimattomuudesta. Verkkolaitteiden valvontaa käsitellään tarkemmin luvussa 2.4.

2.2 Telnet

Verkkolaitteiden etähallinnassa ja -kirjautumisessa on yleisesti käytössä kaksi verkkoprotokollaa Telnet ja SSH, joiden avulla voidaan luoda etäyhteyksiä verkkojen yli laitteisiin ilman, että laitteita joudutaan hallitsemaan paikallisesti laitteiden konsoliportin kautta. Useimmat verkon laitteet ja niiden käyttöjärjestelmät, jotka käyttävät liikennöintiin TCP/IP-verkkoprotokollien (Transmission Control Protocol/ Internet Protocol) yhdistelmää, tukevat Telnetin avulla luotuja etäyhteyksiä (Padmavathi et al. 2012). Telnet-protokolla on määritelty RFC-dokumentissa (Request for Comments) 854.

Telnet on yhteysprotokolla, jonka tarkoituksena on mahdollistaa kaksisuuntainen pääteyhteys tai pääteprosessien käyttö Telnet-yhteyden avulla. Sen pääasiallisena tavoitteena on tarjota rajapinta päätelaitteiden ja pääteprosessien välille. Muodostettu yhteys on TCP-yhteys (Transmission Control Protocol) eli se hyödyntää liikennöidessään TCP-protokollaa. (Postel & Reynolds 1983) Telnet-protokollasta on suuri hyöty esimerkiksi juuri verkkolaitteiden hallinnassa, koska sen avulla voidaan luoda etäyhteyksiä verkkolaitteiden tekstipohjaiseen komentorivikäyttöliittymään Telnet-protokollaa tukevien pääte-emulaattoreiden avulla (Padmavathi et al. 2012). Se toimii siis komentorivipohjaisena yhteysprotokollana ja istunnon muodostamisen jälkeen Telnet-asiakasohjelmiston avulla voidaan esimerkiksi suorittaa komentoja verkon yli hallittavassa laitteessa.

Telnet-protokolla toimii asiakas-palvelin-periaatteella, jossa istunnon aloittaja toimii asiakasosapuolena ja osapuoli, johon yhteys muodostetaan, toimii palvelinosapuolena. Jotta Telnet-istunto voidaan muodostaa kahden osapuolen välille, tulee molemmissa osapuolissa olla niin sanottu virtuaalinen pääte NVT (Network Virtual Terminal). NVT:n tarkoituksena on luoda standardoitu ja yhdenmukainen tiedon esitysmuoto asiakas- ja palvelinosapuolten välille. Näin asiakkaan ja palvelimen ei tarvitse ylläpitää tietoa toistensa

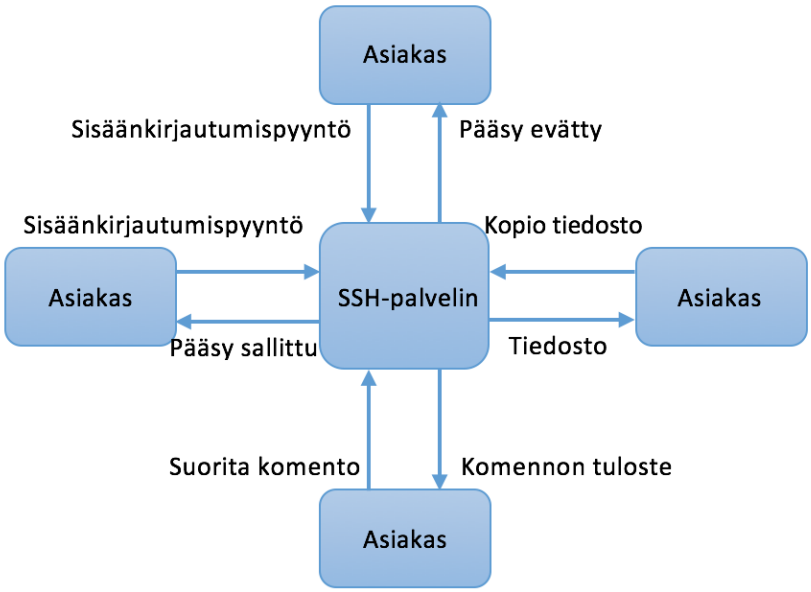
päätteiden ominaisuuksista, vaan molemmat osapuolet muuttavat nämä ominaisuudet NVT-pääteelle sopivaksi. (Postel & Reynolds 1983) Tämä mahdollistaa Telnet-istunnon muodostamisen kahden osapuolen välille riippumatta näiden päätteiden ominaisuuksista. Kun Telnet-istunto muodostetaan, yhteyden asiakasosapuoli aloittaa yhteyden muodostamisen luomalla TCP-yhteyden palvelinosapuoleen. Verkonhallinnan näkökulmasta asiakasosapuolena voi toimia esimerkiksi Telnet-protokollaa tukeva asiakasohjelmisto, jolla otetaan yhteys johonkin verkkolaitteeseen, joka tässä tilanteessa toimii palvelinosapuolena. Yksinkertaistettuna yhteyden asiakasosapuoli lähettää näppäimistöllä syötetyt komennot palvelinosapuolelle muuttaen merkit ensin NVT-päätteille sopiviksi. Palvelinosapuoli vastaavasti lähettää tulosteet takaisin asiakasosapuolelle, jossa lähetetty informaatio tulostetaan terminaaliohjelmiston näytölle. (Zheng & Cui 2010)

Protokollan avulla voidaan siis hallinnoida verkon laitteita luomalla Telnet-istunto hallittavan laitteen kuten esimerkiksi reitittimen tai kytkimen ja Telnet-asiakasohjelmiston välille. Istunto näiden välille voidaan muodostaa, kun verkkolaitteeseen on asetettu hallintaosoite, johon asiakasohjelmistolla otetaan yhteys. Hallintayhteyden avulla päästään käsiksi laitteen resursseihin ja laitetta voidaan hallita esimerkiksi muuttamalla laitteen konfiguraatioita tai laite voidaan uudelleenkäynnistää. Telnet-protokollan heikkoutena voidaan pitää tietoturvan puutetta, koska sellaisenaan protokollassa tiedonsiirto tapahtuu salaamattomana ja selväkielisenä. Tämä aiheuttaa uhkia siirrettäessä esimerkiksi laitteiden salasanoja verkon yli verkkolaitteille, jolloin siirrettävät salasanat kulkeutuvat kohteelle sellaisinaan altistaen näin tiedot kolmannen osapuolen hyökkäyksille (Mahmood 2003). Tästä syystä Telnet-protokollaa ei enää suositella käytettäväksi verkkolaitteiden etäkirjautumisessa, vaan sen tilalle on kehitetty tietoturvallisempia vaihtoehtoja kuten SSH (Peterson & Davie 2012, s. 667-670).

2.3 SSH

SSH-protokollan avulla verkkolaitteiden etähallinta voidaan toteuttaa vastaavalla tavalla kuin Telnet-protokollalla, mutta tietoturvallisin keinoin. RFC-dokumentissa 4251 määritellään, että SSH on protokolla, jonka avulla voidaan turvallisesti kirjautua verkkolaitteille turvattoman verkon yli (Ylönen & Lonvick 2006b). Lisäksi protokolla sisältää myös muita toiminnallisuuksia.

Kuvassa 2.1 on esitetty SSH-protokollan arkkitehtuuri sisältäen kaikki ne toiminnallisuudet, jotka SSH:n asiakas-palvelin-periaatteella ovat mahdollisia.



Kuva 2.1. *SSH-protokollan asiakas-palvelin-arkkitehtuurin mahdollistamat toiminnot (perustuu lähteeseen: Goralski 2009, s. 637).*

Etäkirjautumisen lisäksi protokollan avulla voidaan suorittaa komentoja etälaitteissa sekä siirtää tiedostoja halutulta laitteelta verkkojen yli (Peterson & Davie 2012, s. 667-670).

Pelkistetysti SSH-protokollassa määritellään, kuinka turvallinen tietoliikenneyhteys voidaan muodostaa verkkojen yli. Siinä missä SSH käsittää autentikoinnin, luottamuksellisuuden ja eheyden mahdollistaen näin turvallisen tavan siirtää tietoa, ei Telnet tarjoa samanlaisia keinoja tietoturvan varmistamiseksi. Autentikoinnin tarkoituksena on varmistaa luotettavasti jonkun osapuolen identiteetti eli esimerkiksi, että verkkolaitteeseen voidaan muodostaa yhteys ainoastaan oikeilla tunnistautumistiedoilla. Jokainen SSH-yhteys käsittää kaksi autentikointia. Ensin asiakasosapuoli varmistaa, että SSH-palvelin, johon yhteys halutaan muodostaa, on luotettava. Toinen SSH-yhteyden autentikoinneista on käyttäjäautentikointi, jossa asiakasosapuoli autentikoituu palvelimelle esimerkiksi salasanan avulla. Kun halutaan luoda hallintayhteys verkkolaitteeseen salasana-autentikoinnilla, tulee SSH-protokollaa varten verkkolaitteeseen asettaa salasanat, jotta laitteeseen ei päästä käsiksi ilman tunnistetietoja. Luottamuksellisuus taataan tiedon salauksella eli liikenne SSH-osapuolten välillä salataan, kun se kulkee verkkojen yli. Näin esimerkiksi verkkolaitteiden salasanat eivät kulje verkossa selväkielisinä, mikä on ongelma Telnet-protokollan kohdalla. Tämä luottamuksellisuus perustuu istuntoa varten luotuihin satunnaisiin avaimiin ja salausalgoritmeihin, jotka osapuolet ovat neuvotelleet keskenään. Neuvotelluilla avaimilla ja salausalgoritmeilla salataan liikenne osapuolten välillä koko istunnon ajan. Näiden lisäksi SSH varmistaa myös tiedon eheyden eli, että siirrettävä tieto pysyy muuttumattomana koko tiedonsiirron ajan. Vaikka SSH:n käyttämät alemman protokollatason protokollat tarjoavat omat eheystarkistuksensa, on osaksi SSH-protokollaa

lisätty eheyden varmistus, jolloin tiedonsiirron eheys saadaan varmistettua tehokkaammin. Näiden tietoturvaseikkojen takia SSH-protokollaa suositellaan nykyään käytettäväksi verkkolaitteiden hallintaan ennemmin kuin turvattomampaa Telnet-protokollaa. (Barrett & Silverman 2001, s. 4; Ylönen & Lonvick 2006c; Peterson & Davie 2012, s. 667-670)

Tyypillisin SSH:n käyttökohde verkkolaitteiden hallinnassa on siis etäkirjautumisen mahdollistaminen verkkolaitteelle, kun halutaan esimerkiksi muuttaa laitteen konfiguraatioita. Etäkirjautumisessa SSH toimii Telnetin tapaa asiakas-palvelin-periaatteella, jossa etäyhteys verkkolaitteeseen voidaan muodostaa SSH-asiakasohjelmiston avulla. Istunnon aloittamiseksi muodostetaan näiden kahden osapuolen välille ensin tietoturvallinen tiedonsiirtokanava, jotta kaikki verkossa siirrettävä tieto saadaan salattua. Lopuksi SSH-asiakasohjelmiston avulla autentikoidutaan verkkolaitteelle lähettämällä käyttäjän tunnus ja salasana salattuna SSH-palvelinosapuolelle. Palvelinosapuoli tarkistaa lähetetyt autentikointitiedot ja joko hyväksyy sisäänkirjautumisen laitteelle tai hylkää kirjautumisyrityksen. (Barrett & Silverman 2001, s. 20)

SSH-protokollasta on kehitetty kaksi versiota SSH-1 (SSH version 1) ja SSH-2 (SSH version 2), joista SSH-2 uudempana on tänä päivänä parannuksiensa ansiosta laajemmin käytössä. SSH-2-protokolla käyttää etäkirjautumisessa kahta protokollaa, SSH-TRANS (Secure Shell Transport Layer Protocol) ja SSH-AUTH (Secure Shell Authentication Protocol). SSH-TRANS-protokollan tarkoituksena on luoda eheä, salattu ja siten tietoturvallinen kanava asiakas- ja palvelinosapuolen välille sekä autentikoida palvelinosapuolena toimiva SSH-palvelin (Ylönen & Lonvick 2006b). Samoin kuin Telnet, myös SSH käyttää alemman tason kuljetuskerroksen TCP-protokollaa. SSH-yhteyden muodostuksen ensimmäisessä vaiheessa osapuolten välille luodaan aina SSH-TRANS-kanava, jonka muodostamisen aikana asiakas autentikoi palvelinosapuolen käyttäen RSA-algoritmia (Rivest, Shamir, Adleman). Palvelinosapuoli paljastaa oman identiteettinsä välittämällä oman julkisen avaimensa asiakkaalle. Kun yhteys osapuolten välille on luotu, osapuolet luovat istuntoavaimen, jota käytetään siirrettävän datan salaamiseen koko istunnon ajan. Lisäksi SSH-TRANS-protokollan avulla osapuolet neuvottelevat keskenään salaukseen käytettävän salausalgoritmin. Vastaavasti SSH-AUTH-protokollalla suoritetaan tunnistautuminen palvelimelle, jolloin etäkirjautumisen yhteydessä palvelin joko hyväksyy tai hylkää saapuvat yhteysyritykset riippuen syötetyistä tunnistetiedoista. Yleensä verkkolaitteisiin autentikoidutaan laitteisiin ennalta määritettyjen käyttäjätunnuksen ja salasanan avulla. Toisin kuin Telnetin kohdalla, nyt salasanan lähettäminen palvelimelle on turvallista, koska osapuolten välille on luotu tietoturvallinen tietoliikennekanava, jossa salasanat kulkevat palvelimelle kryptattuina. Palvelinosapuoli tarjoaa asiakasosapuolelle autentikointivaihdoehdot, joiden avulla palvelimelle voidaan autentikoitua. SSH tarjoaa salasana-autentikoitumisen lisäksi vielä kaksi muuta tapaa autentikoitua, julkiseen avaimeen

perustuva autentikoituminen sekä host-based-tunnistautuminen. Yleisin tapa autentikoitua verkkolaitteille on kuitenkin perinteinen tunnus-salasana-yhdistelmä. (Ylönen & Lonvick 2006a; Peterson & Davie 2012, s. 667-670)

2.4 SNMP

Verkkojen monimutkaisuus lisääntyy samalla niiden koon kasvaessa, joten niiden toimintaa on mahdotonta valvoa pelkästään ihmisvoimin. Suuria verkkoympäristöjä varten tarvitaan automatisoituja työkaluja, joiden avulla verkkojen valvontaa voidaan tehostaa. Tämän lisäksi verkot koostuvat yhä enemmän eri laitevalmistajien laitteista ja eri mallisista laitteista, minkä takia on tärkeää, että on olemassa työkalu, jota voidaan hyödyntää erilaisissa verkkoympäristöissä. SNMP on käytetyin verkonhallintastandardi, joka ei ole riippuvainen ympäristöstään. SNMP-termillä ei viitata pelkästään SNMP-protokollaan, vaan siihen liittyy myös muita verkonhallintastandardeja, joiden avulla koko SNMP:n verkonhallinta-arkkitehtuuri voidaan määritellä. (Shin et al. 2007; Stallings 2007, s. 760-763)

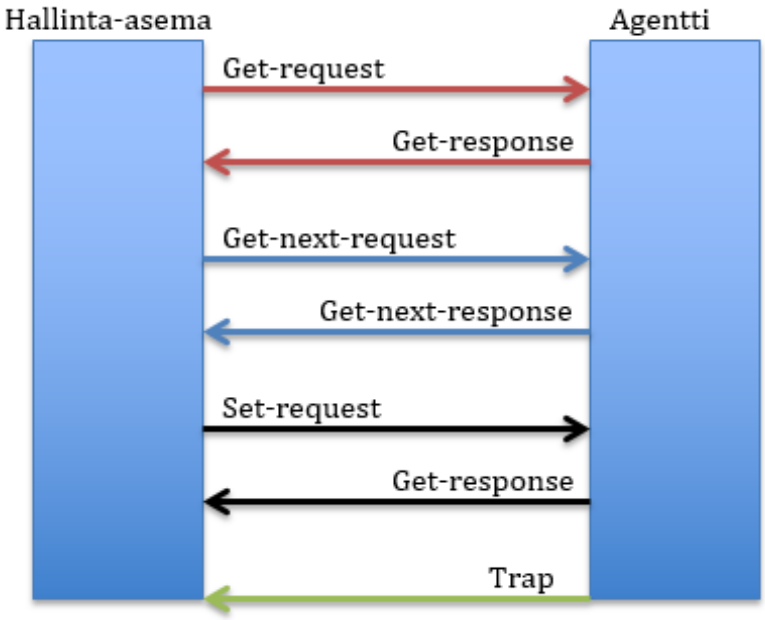
2.4.1 Perustoimintaperiaate

SNMP on kehitetty yksinkertaiseksi verkonhallintastandardiksi, jonka toiminta perustuu kahteen perustoiminnallisuuteen. Sen avulla voidaan valvoa verkkolaitteita tarkkailemalla ja analysoimalla verkkolaitteiden tilaa ja käyttäytymistä, mutta lisäksi sen avulla voidaan myös kontrolloida verkkolaitteita muuttamalla tiettyjä niiden parametreja yksinkertaisia käskyjä suorittamalla (Shin et al. 2007). Verkkolaitteiden valvonta perustuu hallintatietojen tiedusteluun valvottavalta laitteelta, kun taas kontrolloivat toimet perustuvat siihen, että hallittavan laitteen yksittäisten parametrien arvoja voidaan muuttaa vaikuttaen näin laitteen toimintaan. SNMP-verkonhallinta-arkkitehtuuri koostuu kokoelmasta hallinta-asemia sekä hallittavia verkkoelementtejä. Hallinta-asemissa ajettavien hallintaohjelmistojen avulla voidaan valvoa ja kontrolloida verkon laitteita kuten reitittimiä, kytkimiä tai työasemia. (Case et al. 1990) Kokonaisuudessaan SNMP-verkonhallinta-arkkitehtuuri muodostuu viidestä eri peruselementistä, joita ovat hallinta-asemat, hallittavat verkkolaitteet, hallinta-agentit, MIB (Management Information Base) eli verkonhallintamuuttujien tietokanta sekä SNMP-protokolla (Shin et al. 2007; Stallings 2007, s. 760-763).

Hallinta-asema toimii SNMP-arkkitehtuurissa kontrolloivana osapuolena, jonka avulla verkon laitteita voidaan valvoa ja kontrolloida. Hallinta-asema on usein erillinen laite, jossa ajettavalla SNMP-hallintaohjelmistolla voidaan tarjota rajapinta hallittavien järjestelmien ja verkonhallinnasta vastuussa olevien ihmisten välille. SNMP-standardissa on määritelty, että hallinta-asemissa ajettavalla SNMP-sovellusohjelmistolla tulee pystyä valvomaan ja kontrolloimaan verkon laitteita. Lisäksi hallinta-asemaan tulee olla toteutettu tietokanta eli MIB, johon voidaan tallentaa verkkoelementeistä kerättyä tietoa. (Shin

et al. 2007; Stallings 2007, s. 760-763). Niissä verkkoelementeissä, joita SNMP-sovellusohjelmiston avulla hallinnoidaan, on käynnissä SNMP-ohjelmisto, jota kutsutaan agentiksi. Verkon aktiivilaitteet kuten reitittimet ja kytkimet ovat lähes aina varustettu SNMP-agenttiohjelmistolla, jotta laitteita voidaan hallita etälaitteena toimivan hallinta-aseman kautta. Hallittavissa laitteissa agenttien pääasiallisena tehtävänä on lukea hallintamuuttujien arvoja ja tarkkailla niissä tapahtuvia tilamuutoksia. Tämän lisäksi agenttien tehtävänä on suorittaa hallinta-asemien pyytämät hallintatoimet eli muuttaa parametrien arvoja hallinta-asemilta lähetettyjen pyyntöjen mukaan. Agentit voivat myös välittää hallinta-asemalle hallintatietoja ilman, että nämä toimet vaativat hallinta-asemalta minkäänlaisia toimia. (Case et al. 1990; Stallings 2007, s. 760-763)

SNMP-arkkitehtuurissa on käytössä kolme hallintaoperaatiota: parametrien tiedustelu (get), parametrien määrittäminen (set) sekä tapahtumista ilmoittaminen (notify), jota usein kutsutaan myös ansaksi (trap) (Stallings 2007, s. 760-763). Kuvassa 2.2 on havainnollistettu hallinta-aseman ja agentin väliset hallintaoperaatiot ja tiedonvälitykset, jotka on alun perin määritelty SNMP:n ensimmäisessä versiossa SNMPv1 (Simple Network Management Protocol version 1).



Kuva 2.2. *SNMPv1 hallinta-aseman ja agentin väliset operaatiot ja tiedonvälitys (perustuu lähteeseen: Shin et al. 2007, s. 335).*

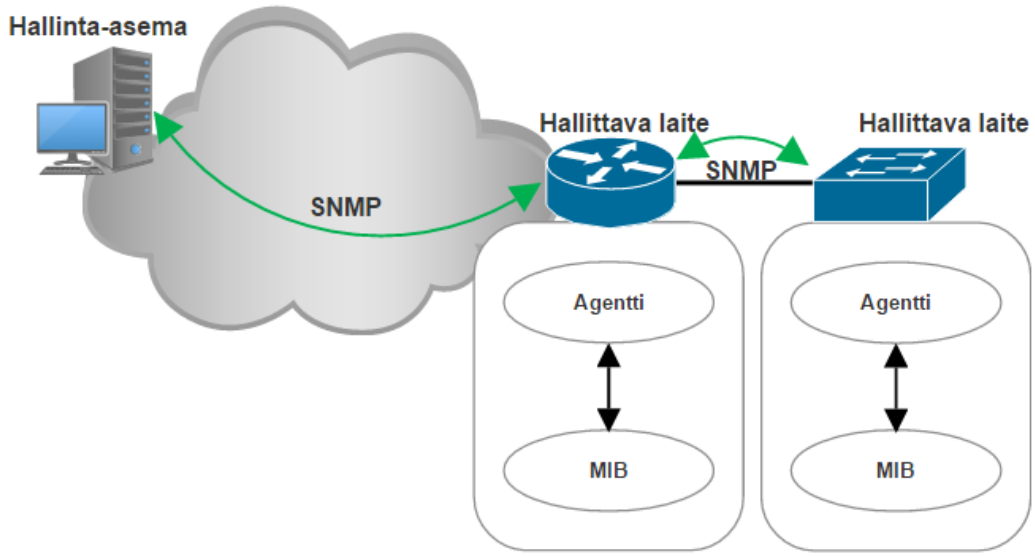
Kuvan 2.2 kahdessa ensimmäisessä operaatiossa on kyse parametrien tiedustelusta, joissa hallinta-asema tiedustelee verkkolaitteen, jossa on käynnissä agenttiohjelmisto tietyn parametrin arvoa. Tähän tiedusteluun agentti vastaa välittämällä hallinta-aseman pyytämän parametrin arvon takaisin hallinta-asemalle. Kolmannessa operaatiossa eli parametrien määrittämisessä hallinta-asema voi muuttaa agenttilaitteen tietyn objektin parametrin arvoa, jonka asettamisen agentti kuittaa tehdyksi hallinta-asemalle. Näissä kolmessa ensimmäisessä operaatioissa käytetään niin sanottua pollausmenetelmää eli kiertokyselyä, jossa

hallinta-asema välittää agentille pyynnön, jonka suorituksen agentti kuittaa takaisin hallinta-asemalle. Kuvan 2.2 viimeisessä operaatiossa (trap) agentti informoi hallinta-asemaa tietystä tapahtumasta, joka on tapahtunut agenttilaitteessa. Agentti välittää tilatiedon hallinta-asemalla, kun verkkolaitteessa tapahtuu jokin merkittävä tilamuutos tai kun laitteen jokin hallintaparametri saavuttaa tietyn arvon. Esimerkiksi agentti voi informoida hallinta-asemaa verkkolaitteen porttien tilamuutoksista. Tässä operaatiossa tiedonvälitys on yksisuuntaista eli ainoastaan agentti välittää tietoa hallinta-asemalle ilman, että hallinta-aseman tarvitsee esittää pyyntöä agentille. (Shin et al. 2007; Stallings 2007, s. 760-763)

Jotta tiedetään, minkä parametrin arvoa hallinta-asema haluaa tiedustella agenteilta tai vaihtoehtoisesti minkä parametrin arvon se haluaa agenttilaitteelle määrittää, tarvitaan tietokanta, jossa verkkolaitteiden ja verkon tilaa kuvaavien parametrien arvoja säilytetään. Tätä tarkoitusta varten osana SNMP-arkkitehtuuria on MIB-tietokanta eli verkonhallintamuuttujien tietokanta, johon tallennetaan verkkolaitteiden hallinnassa tarvittavien parametrien arvoja. Hallittavat resurssit voidaan nähdä kokoelmana hallittavia objekteja, joiden arvot on tallennettu virtuaaliseen tietovarastoon. Kaikki tietokannassa olevat objektit ovat itse asiassa muuttujia, joista jokainen kuvaa jollakin tapaa hallittavan laitteen tai verkon tilaa. Molemmissa niin hallinta-asemissa kuin agenteissa on omat tietokantansa, joissa säilytetään objektien senhetkisiä arvoja. Verkkolaitteiden hallinta perustuu pääasiassa näiden objektien arvojen käsittelyyn. Kun hallinta-asema haluaa tiedustella tai määrittää tietyn objektin arvon, agenttiohjelmisto vastaanottaa tiedustelupyynnön hallinta-asemalta ja joko lukee muuttujan arvon tietokannastaan tai käy muuttamassa muuttujan arvon tietokantaansa ja kuittaa operaation tehdyksi takaisin hallinta-asemalle kuvan 2.2 mukaisesti. (Stallings 2007, s. 760-763; McCloghrie et al. 1999)

SNMP-protokollan tehtävänä on mahdollistaa kommunikointi hallinta-asemien ja verkkolaitteissa toimivien agenttiohjelmistojen välillä (Case et al. 1990). SNMP-protokolla on sovellustason protokolla, joka kuuluu TCP/IP-protokollasarjaan. Tavallistesti se käyttää liikennöintiin alemman tason protokollista UDP- (User Datagram Protocol) ja IP-protokollia (Internet Protocol), mutta voi tietyissä tilanteissa toimia UDP:n sijaan myös TCP-protokollan avulla. Niin hallinta-asemissa kuin agenteissa on käynnissä omat SNMP-prosessinsa, joiden tehtävänä on käsitellä niiden omia MIB-tietokantoja. Hallinta-asemissa käynnissä oleva hallintaprosessi kontrolloi pääsyä sen omaan keskustietokantaan ja tarjoaa mahdollisuuden verkkolaitteiden hallintaan SNMP-protokollan avulla. Agenttilaitteissa on käynnissä vastaavanlainen prosessi, joka hallintaprosessin tavoin käyttää SNMP-protokollaa hallinnoiden näin etäyhteyksiä sen omaan MIB-tietokantaan. (Stallings 2007, s. 760-763)

Kuvassa 2.3 on esitetty yksinkertainen mallinnus SNMP-protokollan toimintaperiaatteesta osana verkkolaitteiden hallintaa.



Kuva 2.3. *Havainnollistus verkkolaitteiden hallinnasta SNMP:n avulla (perustuu lähteeseen: Nadeau 2003, s. 62).*

Kuvassa 2.3 on kaksi etäältä hallittavaa laitetta, yksi reititin ja yksi kytkin, joissa molemmissa on käynnissä SNMP-agenttiohjelmisto, joiden kautta laitteita voidaan hallita fyysisesti etäällä olevan hallinta-aseman avulla. Hallinta-asemalta voidaan tiedustella SNMP-protokollaa käyttäen esimerkiksi kytkimen käynnissäoloaika lähettämällä hallinta-asemalta SNMP-pyyntö hallittavalle laitteelle. Hallittavilla laitteilla käynnissä oleva agenttiprosessi pitää yllä tietokantaa hallittavista objekteista. Kun hallittava laite vastaanottaa saapuneen SNMP-viestin, käsittelee agenttiprosessi pyynnön tarkistamalla pyydettyjen objektien arvot MIB-tietokannasta ja lopuksi kokoaa näistä tiedoista SNMP-viestin, joka välitetään takaisin hallinta-asemalle. (Nadeau 2003, s. 61-62) Vaihtoehtoisesti hallittavat laitteet voivat lähettää hallinta-asemalle trap-viestin, mikäli laitteille on ennalta määritetty ansat, joiden toteutumisesta laitteiden tulee lähettää ilmoitus hallinta-asemalle.

2.4.2 SNMPv2 ja SNMPv3

SNMP-standardin ensimmäinen versio SNMPv1 on alun perin kehitetty yksinkertaiseksi verkonhallintatyökaluksi, jonka avulla voidaan saavuttaa tehokas ja valmistajariippumaton verkonhallintaympäristö varsinkin TCP/IP-pohjaisten verkkojen hallintaan. Arkkitehtuurin verrattain yksinkertainen toteutus on mahdollistanut sen laajan käytön ja tämän ansiosta SNMP:sta on tullut käytetyin verkonhallintastandardi. Vähitellen verkkojen monimutkaistuttua ja laajennuttua, alkoi sen ensimmäinen versio paljastaa heikkouksia ja puutteitta, jonka takia SNMP-standardin kehitystä on myöhemmin jatkettu uudemmilla versioilla, jotta sen avulla voitaisiin vastata nykyisten verkkojen lisääntyneisiin vaatimuk-

siin. (Stallings 1998) Kaikki SNMP-standardin versiot SNMPv1, SNMPv2 (Simple Network Management Protocol version 2) sekä SNMPv3 (Simple Network Management Protocol version 3) sisältävät samanlaisen perusrakenteen ja samat komponentit (Case et al. 1999).

Ensimmäisen version suurimpia puutteita ovat hallinta-asemien välisen kommunikaation puute, puute siirtää suuria hallintatietomääriä kerralla sekä tietoturvan puute. SNMP-standardin toinen versio SNMPv2 toi toiminnallisia parannuksia edeltävään versioon niin tiedonsiirron tehokkuuden kuin hallinta-asemien välisen kommunikaation osalta, mutta ei ratkaissut ensimmäisen version tietoturvapuutteita, mikä on suurin syy siihen, minkä takia SNMPv2 ei ole saanut laajempaa suosiota. Suurimpana yksittäisenä parannuksena SNMPv2 on tuonut mahdollisuuden siirtää suurempia määriä hallintatietoja kerralla hallinta-asemien ja agenttien välillä vähentäen näin protokollaliikennettä osapuolten välillä. Kun ensimmäisessä versiossa on mahdollista siirtää kerralla ainoastaan pienempiä tietomääriä hallinta-asemien ja agenttien välillä, joudutaan hallinta-asemalta välittämään useita yksittäisiä pyyntöjä agenteille, kun halutaan tiedustella useampien objektien arvoja aiheuttaen näin enemmän edestakaista liikennettä osapuolten välillä. SNMPv2:ssa tämä ongelma on ratkaistu mahdollistamalla useamman objektin arvon tiedustelu yhdellä hallinta-aseman get-pyynnöllä. Näiden SNMPv2:n GetBulk-pyyntöjen avulla voidaan siis vähentää yksittäisten get-pyyntöjen lähettämistä hallinta-asemilta parantaen hallinnan tehokkuutta. SNMPv2:n toinen merkittävä parannus on hajautetun hallinnan ja hallinta-asemien välisen liikennöinnin mahdollistaminen. Hajautetulla hallinnalla tarkoitetaan useamman hallinta-aseman muodostamaa hallintakokonaisuutta, jossa voi olla useampia ylemmän tason hallinta-asemia, jotka ovat vastuussa tiettyjen agenttien hallinnoimisesta. Toisaalta hajautetussa hallinnassa näiden ylemmän tason hallinta-asemien lisäksi on alemman tason hallinta-asemia, jotka ovat viimekädessä vastuussa agenttien valvonnasta ja kontrolloinnista. Alemman tason hallinta-asemia voidaan hallinnoida ylemmän tason hallinta-asemilla, jolloin alemman tason hallinta-asemat toimivat agentin roolissa ylemmän tason hallinta-asemille. Hajautuksella vältetään yhden keskitetyn hallinta-aseman kuormitus, jolloin kaikki hallintaliikenne ei kohdistu yhdelle hallinta-asemalle, vaan useiden agenttien hallintatietojen aiheuttama liikenne voidaan jakaa tasaisesti usealle hallinta-asemalle. SNMPv2 mahdollistaa lisäksi hallinta-asemien välisen liikennöinnin, joka auttaa muun muassa mahdollisten vikatilanteiden havainnoimista ja niistä ilmoittamista. Hallinta-asemat voivat välittää toisilleen viestin, kun esimerkiksi jokin epätavallinen tapahtuma ilmenee. (Stallings 1998)

Kahden ensimmäisen SNMP-version suurimpana puutteena ollut tietoturvallisuuden puute on onnistuttu korjaamaan SNMP:n kolmannessa versiossa. SNMPv3 tuo SNMP-standardiin uusina ominaisuuksina autentikoinnin, salauksen ja pääsynvalvonnan. Muutoin SNMPv3:n voidaan sanoa sisältävän samat toiminnalliset ominaisuudet kuin jo sitä edeltävässä SNMPv2:ssa. Uusista turvallisuusominaisuuksista autentikointi sallii pyyn-

nöt ainoastaan valtuutetuilta hallinta-asemilta. Lisäksi osana autentikointia agentti tarkistaa, ettei hallinta-asemilta lähetettyjä pyyntöjä ole muutettu. Autentikoinnin tuomat ominaisuudet agenttien ja hallinta-asemien välillä on toteutettu jaettujen salausavaimien avulla. Avainten avulla laskettujen tarkistussummien avulla voidaan vahvistaa viestin muuttumattomuus, jolla voidaan samalla varmistua siitä, että pyynnöt on lähetetty valtuutetulta hallinta-asemalta. Salaus mahdollistaa hallinta-asemien ja agenttien välisen liikenteen salaamisen jaettujen salausavaimien avulla. Tällä saavutetaan tietoturvallinen liikennöinnin näiden osapuolten välillä. Agenttilaitteiden resursseihin voidaan konfiguroida erilaisia pääsynvalvontarajoituksia, jotka määrittelevät sen, mitkä hallinta-asemat pääsevät mihinkin agenttilaitteiden resursseihin käsiksi. Jokaiselle hallinta-asemalle voidaan määrittää agenttilaitteisiin omat pääsynvalvontarajoitukset rajoittaen näin tiettyjen hallinta-asemien hallinnointioikeuksia. (Stallings 1998)

2.5 Hallintaosoitteen määritelmä

Jotta verkkolaitteiden hallinta ja valvonta voidaan toteuttaa etäyhteyksien avulla, tulee jokaiselle hallintaan ja valvontaan otettavalle laitteelle määrittää erillinen hallintaliitäntä. Hallintaliitännät mahdollistavat verkkojen ylläpidosta vastuussa olevien henkilöiden pääsyn hallinnoimaan verkon laitteita heidän omista verkoistaan. Hallintaliitäntöjen kautta verkon ylläpitäjät pääsevät kontrolloimaan verkon laitteita, tarkastelemaan konfiguraatioita ja lukemaan laitteiden tilatietoja. (Nadeau 2003, s. 28) Hallintayhteyksien kannalta hallintaliitäntöjen tarkoituksena on muun muassa mahdollistaa etäkirjautuminen laitteelle Telnet- ja SSH-protokollien avulla, jolloin laitetta voidaan hallita milloin ja mistä tahansa. Lisäksi SNMP-protokolla hyödyntää samaa hallintaliitäntää kerätäkseen tietoa hallittavalta laitteelta. Jokaiselle hallinnassa olevalle laitteelle niin reitittimelle kuin kytkimelle sen hallintaliitännälle tulee määrittää IP-osoite, joka määrittää sen kohteen, johon laitteen hallinta tai valvonta halutaan kohdistaa. Jatkossa tässä työssä vastaaviin osoitteisiin viitataan termillä hallintaosoite, joka määrittelee laitteen tietyn liitännän, jonka kautta laitteen hallinta- ja valvontayhteydet saapuvat laitteelle.

Verkkoreitittimien hallinta tapahtuu fyysisten verkkoliitäntöjen kautta, jolloin laitteen tietylle liitännälle, joka yhdistää laitteen laajempaan verkkoympäristöön tai oikeastaan sen aliliitännälle (subinterface), asetetaan hallintaa varten IP-osoite. Tämän liitännän kautta hallinta- ja valvontayhteydet saapuvat laitteelle. Kytkimien hallinta ei tapahdu samalla tavalla fyysisten liitäntöjen kautta, vaan niiden hallinta tapahtuu tyypillisesti virtuaalisesti lähiverkkojen VLANien (Virtual Local Area Network) kautta. Tällöin kytkimelle tulee ensin luoda hallintaa varten oma virtuaalinen lähiverkko eli VLAN. Lisäksi laitteelle tulee luoda hallintaa varten myös VLAN-liitäntä, jolle asetetaan IP-osoite. Hallintaa varten luotu virtuaalinen liitäntä liitetään osaksi laitteen fyysistä liitäntää, jolloin virtuaaliseen lähiverkkoon kuuluva liikenne sallitaan kyseisen fyysisen portin kautta laitteelle. Hallintaan tarkoitetun virtuaalisen lähiverkon liikenteen salliminen mahdollistaa hallinta- ja

valvontatyökalujen avulla laitteelle muodostetut yhteydet. Työn tutkimusosassa on tarkoitus tutkia näiden osoitteiden soveltuvuutta hallintaan ja valvontaan, kun hallintaosoitteina käytetään perinteisten IPv4-osoitteiden sijaan uudemman protokollaversion IPv6-osoitteita.

3. IPv6 OSANA VERKKOLAITTEIDEN HALLINTAA JA VALVONTAA

Tässä luvussa käsitellään IPv6-osoitteistusta yleisesti, tuodaan esille IPv4- ja IPv6-osoitteiden eroja sekä esitellään IPv6-protokollan osoitetyypit. Lisäksi luvussa käsitellään IPv6-protokollan ominaisuuksia ja mahdollistamia toimintoja niiltä osin kuin ne tämän työn ja myöhemmässä vaiheessa käsiteltävien laboratorioympäristössä suoritettavien tutkimusten kannalta on tarpeellista. Tarkoituksena on tuoda esille niitä protokollan ominaisuuksia ja toimintoja, joilla on merkitystä verkkolaitteiden hallinnan ja valvonnan kannalta.

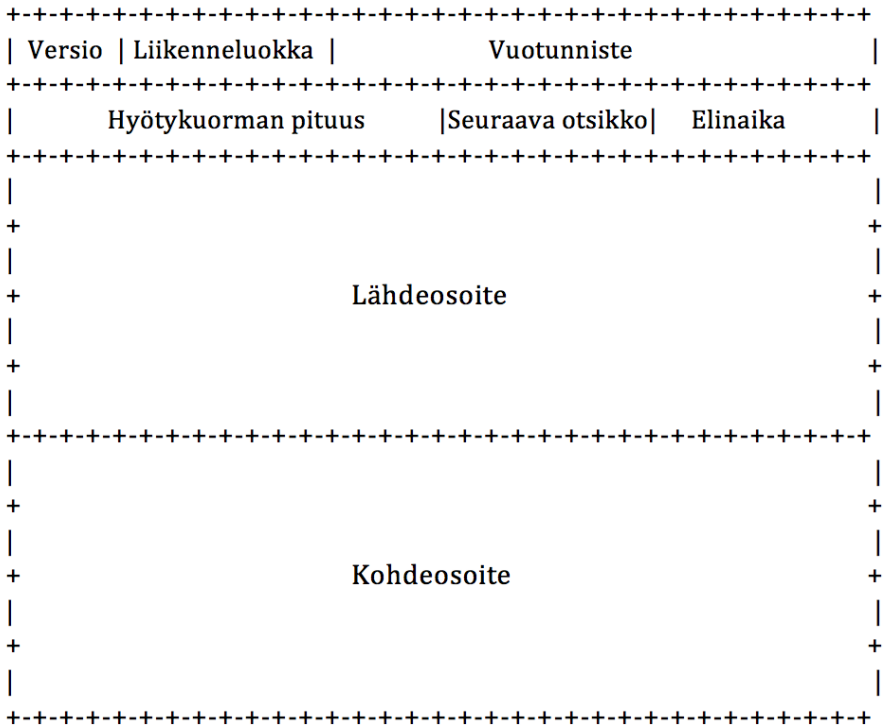
3.1 IPv6-osoitteistus yleisesti

Uusi IP-protokolla on tuonut joitakin merkittäviä muutoksia protokollan toteutukseen ja samalla mahdollistanut uusia ominaisuuksia, jotka eivät ole toteutettavissa vanhemmalla IPv4-versiolla. IPv6-protokollan merkittävin yksittäinen muutos sitä edeltävään versioon nähden on osoiteavaruuden kasvattaminen IPv4:n 32-bittisistä osoitteista IPv6:n 128-bittisiin osoitteisiin, mikä teoriassa tarkoittaa $3{,}4 * 10\text{^}38$ mahdollista IPv6-osoitetta (Peterson & Davie 2012, s. 327). Laajennetun osoiteavaruuden ansiosta IPv6-osoitteiden loppuminen IPv4-osoitteiden tapaan ei ole samalla tavalla mahdollista. Toinen selkeä ero protokollien toteutuksissa on havaittavissa IP-pakettien otsikkorakenteissa. IPv6-paketin otsikkorakennetta on muutettu selvästi IPv4-paketin otsikkorakenteeseen verrattuna poistamalla kokonaan osa siihen kuluvista kentistä yksinkertaistaen näin koko otsikkorakennetta. Lisäksi osa IPv4-paketin otsikkorakenteeseen kuuluvista kentistä IPv6-protokollan tapauksessa on siirretty osaksi paketin laajennusosaa, eivätkä ne siksi ole pakollinen osa IPv6-otsikkorakennetta. (Deering & Hinden 1998; Kurose & Ross 2008, s. 386-389)

Alla olevissa kuvissa on vertailun vuoksi esitetty molempien protokollien, IPv4- ja IPv6-pakettien otsikkorakenteet. Ensin kuvassa 3.1 on esitetty IPv4-protokollan otsikkorakenne.

Kuva 3.1. *IPv4-paketin otsikkokentät (perustuu lähteeseen: Postel 1981, s. 11).*

Kuvassa 3.2 on vastaavasti esitetty IPv6-paketin rakenne otsikkokenttien osalta.



Kuva 3.2. *IPv6-paketin otsikkokentät (perustuu lähteeseen: Deering & Hinden 1998, s. 4).*

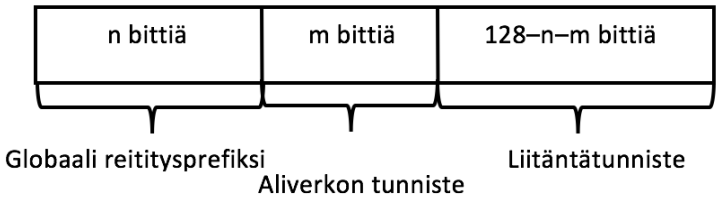
Kuvissa yksi rivi vastaa neljää tavua eli 32 bittiä. Kuten kuvista 3.1 ja 3.2 huomataan, on IPv6-protokollan kehysrakenne otsikkokenttien osalta yksinkertaisempi sisältäen vähemmän yksittäisiä kenttiä. IPv6-protokollassa yksinkertaisemman otsikkorakenteen tavoitteena on ollut suoraviivaistaa pakettien käsittelyä mahdollistaen näin nopeammat pakettien prosessointiajat verkon solmupisteissä. Siinä missä IPv6-paketin otsikkorakenteessa on kahdeksan tavua otsikkotietoja ennen 128-bittisiä lähde- ja kohdeosoitteita, on IPv4-paketin otsikkorakenteessa vastaavasti 12 tavua otsikkotietoja ennen osoitteita. Osa IPv4-paketin otsikkokentistä on sisällytetty edelleen IPv6-pakettiin, mutta osa kuten tarkistussumma, fragmentointiin liittyvät kentät sekä lisäoptiot on poistettu. IPv6-paketin otsikkorakenteesta on saatu kiinteänmittainen poistamalla otsikkotiedoista lisäoptiokentät. Koska IPv6-paketit voivat sisältää vaihtelevan määrän lisäoptiokenttiä, on ne siirretty pois niin sanotusta pääotsikkorakenteesta IP-paketin ja seuraavan tason protokollan otsikkorakenteen väliin, jolloin ne eivät vaikuta pääotsikkorakenteen kokoon. Tämän yksinkertaistuksen ansiosta IPv4-otsikkorakenteessa esiintyvää otsikon pituus -kenttää ei IPv6-protokollassa enää tarvita, vaan lisäoptiokenttien olemassaolo ilmaistaan otsikkorakenteen seuraava otsikko -kentän avulla. Poistamalla tarkistussumma paketin otsikkorakenteesta, on IPv6-pakettien välitys verkossa saatu nopeammaksi, koska enää jokaisessa verkon reitityspisteessä ei tarvitse laskea ja päivittää tarkistussummaa. Tarkistussummakentät on voitu poistaa paketin otsikkorakenteesta, koska on ajateltu, että ylemmän protokollatason protokollat kuten TCP ja UDP suorittavat paketeille omat tarkistussumman laskennat, joten tarkistussumman laskentaa voidaan IP-tasolla pitää tarpeettomana. IPv6-paketin otsikkorakenteesta on jätetty kokonaan pois myös fragmentointiin liittyvät tavut eli yhteensä 4 tavua, jotka kuvassa 3.1 sijaitsevat toisella rivillä. IPv6-protokollassa vastuu pakettien koon selvittämisestä on siirretty päätelaitteille, eikä verkon laitteille IPv4-protokollan tavoin. Tällä saavutetaan se, ettei IPv6-protokollassa tarvita fragmentointikenttiä, koska paketin lähettävä laite selvittää PMTUD-menetelmän (Path Maximum Transmission Unit Discovery) avulla sopivan pakettikoon, joka voidaan siirtää lähde- ja kohdelaitteen välillä. Samoin kuin tarkistussumman laskenta myös fragmentoinnin poistaminen verkkolaitteilta vähentää verkkolaitteiden kuormitusta nopeuttaen näin pakettien prosessointia. (Huitema 2000, s. 63-66; Kurose & Ross 2008, s. 386-389)

3.2 Unicast-osoitteet

Uuden protokollan myötä myös IP-osoitteistus on muuttunut hieman. IPv6-protokollassa sallitaan, että verkkolaitteiden liitännät voidaan identifioida erilaisten IP-osoitteiden avulla helpottaen näin reititystä ja hallintaa. (Huitema 2000, s. 56) RFC-dokumentissa 4291 on määritelty IPv6-osoitteistuksen kolme osoitetyyppiä, jotka jakavat osoitteet kolmeen eri pääluokkaan. Jokainen IPv6-osoite kuuluu johonkin seuraavista osoitetyypeistä unicast, multicast tai anycast. (Deering & Hinden 2006) Eri osoitetyyppien tarkoituksena on määrittää, viitataanko yksittäisellä osoitteella yhteen tiettyyn verkkolaitteen liitäntään

vai esimerkiksi useamman verkkolaitteen liitäntöihin. Toisin sanoen osoitetyyppi määrittää, onko tietyn osoitetyypin osoitteella varustettu paketti tarkoitus välittää yhteen tiettyyn IP-osoitteella yksilöityyn kohteeseen vai useampaan kohteeseen.

Unicast-osoitteet kuvaavat perinteisiä pisteestä-pisteeseen-osoitteita, jotka identifioivat yksittäisen verkon liitännän osoitteen. Kun paketti lähetetään unicast-osoitteeseen, voidaan olettaa, että lähetetty paketti välittyy juuri siihen liitäntään, jonka tämä kyseinen unicast-osoite yksilöi. IPv6-protokollassa unicast-osoitteet on edelleen jaoteltu erityyppisiin osoitteisiin, joilla jokaisella on omat käyttötarkoituksensa IPv6-osoitearkkitehtuurissa. Erityisesti globaalit unicast-, link-local- ja site-local-osoitteet ovat uusia IPv6-protokollan ominaisuuksia, eivätkä siten esiinny sellaisinaan IPv4-protokollassa. Erityyppisillä unicast-osoitteilla on omien käyttötarkoituksiensa lisäksi myös erilaiset vaikutusalueensa. Tässä osoitteiden vaikutusalueella tarkoitetaan verkon aluetta, joka määrittelee, kuinka laajasti tietyntyyppisellä unicast-osoitteella voidaan osoittaa. Yleisesti unicast-osoitteet muodostuvat sisäisen rakenteen osalta hierarkkisesti muodostaen lopulta koko 128-bittisen osoiterakenteen. (Deering & Hinden 2006) Esimerkiksi globaalien unicast-osoitteiden koko osoiterakenne muodostuu yleisesti kuvassa 3.3 esitetyllä tavalla.

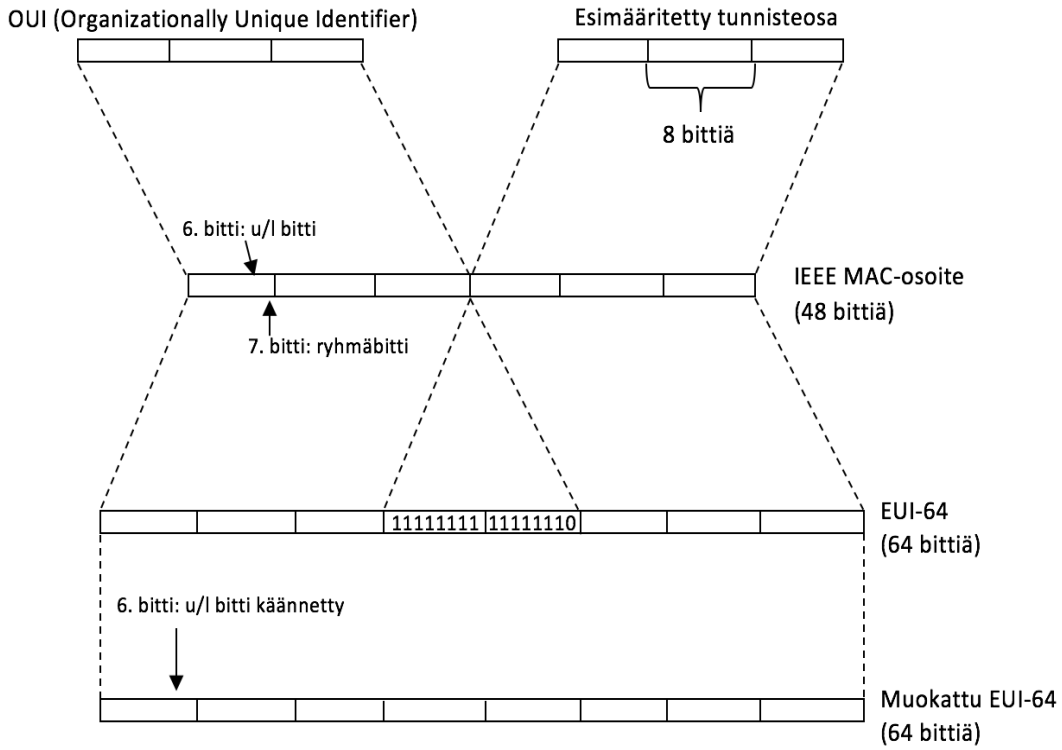


Kuva 3.3. *Tyypillinen globaalin IPv6-unicast-osoitteen rakenne (perustuu lähteeseen: Deering & Hinden 2006, s. 9).*

Jokaisen verkkoon liitetyn laitteen joko fyysinen tai looginen liitäntä on osa jotakin aliverkkoa, jolloin kyseisen liitännän osoite koostuu aliverkon prefiksistä ja laitteen yksilöivästä liitäntätunnisteesta. Käytännössä siis IPv6-osoitteet muodostuvat kahdesta osasta: verkko-osasta ja liitännän yksilöivästä liitäntätunnisteesta. Aliverkon prefiksi taas usein muodostuu kahdesta osasta, verkon tunnisteesta eli globaalista reitityksprefiksistä ja aliverkon tunnisteesta. (Huitema 2000, s. 58) Globaalit reitityksprefiksit ovat hierarkkisesti verkoille asetettuja ja hallittuja tunnisteita, joiden hallinnasta RIR-järjestöt (Regional Internet Registry) ja Internet-palveluntarjoajat ovat vastuussa (Hinden et al. 2003). Unicast-osoitteet ovat reititettäviä, joiden reititys perustuu mielivaltaisen pituiseen globaaliin reitityksprefiksiin. (Deering & Hinden 2006)

Kuvan 3.3 globaalin unicast-osoitteen liitäntätunnistetta käytetään siis yksilöimään aliverkon tietty liitäntä. Saman aliverkon tunnisteen alla ei voi olla kahta samalla liitäntätunnisteella olevaa liitäntää. Toisin sanoen samassa aliverkossa ei saa olla kahta samalla

MAC-osoitteella (Media Access Control) olevaa liitäntää, koska yleensä 64-bittinen liitäntätunnus johdetaan liitännän MAC-osoitteesta. Toisaalta samaa liitäntätunnusta voidaan käyttää useammassa laitteen liitännässä, mikäli nämä liitännät vain kuuluvat eri aliverkkoihin. Protokollassa hyödynnetään IEEE:n (Institute of Electrical and Electronics Engineers) määrittelemää muokattua EUI-64-menetelmää (Extended Unique Identifier) unicast-osoitteen liitäntätunnisteen muodostamiseen. Deeringin ja Hindenin (2006) määrittelemässä RFC-dokumentissa 4291 sanotaan, että kaikilla unicast-osoitteilla lukuun ottamatta niitä, jotka alkavat binääriarvolla 000 on oltava 64-bittinen liitäntätunniste, jonka tulee olla muokatussa EUI-64-muodossa. Binääriarvolla 000 alkavilla osoitteilla ei ole vastaavaa rajoitusta liitäntätunnisteen pituudessa. IPv6-protokollassa liitäntätunnus muodostetaan siis normaalisti liitännän 48-bittisen MAC-osoitteen perusteella. Käytännössä tämä tapahtuu siten, että 48-bittisen MAC-osoitteen kolmannen ja neljännen tavun väliin lisätään erityinen 16-bittinen binääriarvo (11111111 11111110), joka täydentää MAC-osoitteen 64-bittiseksi liitäntätunnisteeksi. Kuvassa 3.4 on esitetty havainnollistus, kuinka liitännän MAC-osoitteesta voidaan muodostaa 64-bittinen EUI-64- ja edelleen muokattu EUI-64-liitäntätunnus.

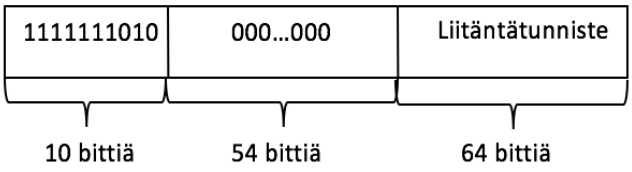


Kuva 3.4. *Havainnollistus, kuinka MAC-osoite muutetaan EUI-64- muotoon ja edelleen muokattuun EUI-64-muotoon (perustuu lähteeseen: Beijnum 2006, s. 17).*

Edellä olevassa kuvassa on ensin esitetty alkuperäisen 48-bittisen MAC-osoitteen rakenne, joka yleisesti koostuu kahdesta 24-bittisestä osasta. Osoitteen alkupää muodostuu

OUI-tunnisteesta (Organizationally Unique Identifier), joka on yleensä tietyn organisaation yksilöivä tunniste. Tämän perässä on 24-bittinen tunnisteosa, jonka valmistajaorganisaatio määrittää yksilöimään MAC-osoitteen. OUI-tunnisteen ensimmäisen tavun kaksi viimeistä bittiä on varattu erilliseen tarkoitukseen. Kuudes bitti (u/l-bitti) ilmaisee, onko MAC-osoite globaalisti uniikki vai ei. Seitsemäs bitti eli ryhmäbitti (group bit) määrittää, onko osoite multicast-osoite vai tavallinen unicast-osoite. Kun MAC-osoitteen OUI-tunnisteen ja esimääritetyn tunnisteosan väliin lisätään 16-bittinen edellä mainittu binääriluku, saadaan EUI-64-tunniste, jonka pituus on 64-bittiä. Kun tämän osoitteen u-bitti vielä käännetään, saadaan muokattu EUI-64-tunniste. Muokatussa EUI-64-tunnisteessa u/l-bitin ollessa yksi, on liitäntätunniste globaalisti uniikki ja vastaavasti sen ollessa nolla on osoite paikallinen. (IEEE Standards Association 1997; Deering & Hinden 2006; Beijnum 2006, s. 16-17)

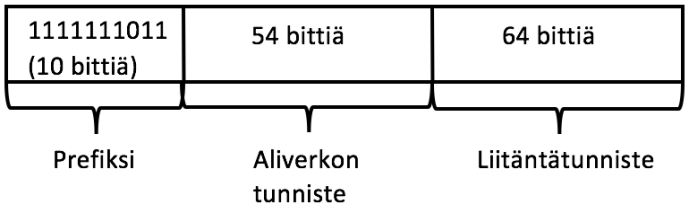
IPv6-protokollassa on määritelty lisäksi kaksi paikalliseen käyttöön tarkoitettua osoitetyyppiä link-local- ja site-local-osoitteet. Link-local-osoitteet ovat rajoitettu käytettäväksi yhden paikallisen linkin vaikutusalueella. Osoitteita voidaan käyttää siis ainoastaan naapurilaitteiden väliseen kommunikointiin. Tällöin laitteille ei ole vielä asetettu globaalia unicast-osoitetta tai laitteet eivät ole saaneet sitä vielä automaattisen konfiguroinnin avulla. On määritelty, että jokaisen verkkolaitteen aktiivisella IPv6-protokollaa käyttävällä liitännällä tulee olla vähintään tällainen osoite, jota käytetään pääasiallisesti alustukseen liittyvissä operaatioissa. Osoitteita käytetään muun muassa NDP:n (Neighbor Discovery Protocol) eli ND-protokollan ja erityisesti automaattisen konfiguroinnin yhteydessä. Kuvassa 3.5 on esitetty link-local-osoitteen rakenne.



Kuva 3.5. *Link-local-osoitteen rakenne (perustuu lähteeseen: Deering & Hinden 2006, s. 11).*

Kuvan 3.5 mukaan link-local-osoitteet muodostuvat vakiona pysyvästä prefiksistä, sarjasta nollia ja liitäntätunnisteesta. Vakiona pysyvä prefiksi nollabittien kanssa heksamuotoiseksi muutettuna saa muodon FE80::/64, joka täydennetään 128-bittiseksi link-local-osoitteeksi lisäämällä tämän perään 64-bittinen liitäntätunniste. Osoitteen yksilöi sisäisen rakenteen lopussa oleva 64-bittinen liitäntätunniste, jonka muodostamiseen hyödynnetään yleensä verkkolaitteen liitännän MAC-osoitetta. Reitittimet eivät koskaan välitä eteenpäin paketteja, joissa link-local-osoitteet ovat joko lähde- tai kohdeosoitteina, vaan osoitteet ovat voimassa ainoastaan siinä paikallisessa linkissä, johon niitä mainostetaan, eikä niitä siten voida käyttää laajempaan välitykseen. (Brown 2002, s. 133-135; Deering & Hinden 2006)

Kolmas unicast-osoitetyyppi on site-local-osoitteet, joita voidaan käyttää sisäverkon osoitteistukseen ilman globaalia prefiksiä, kun halutaan, ettei osoitteita reititä julkiseen verkkoon. Site-local-osoitteet noudattavat myös tiettyä sisäistä rakennetta. Kuvassa 3.6 on esitetty tällaisen site-local-osoitteen sisäinen rakenne.



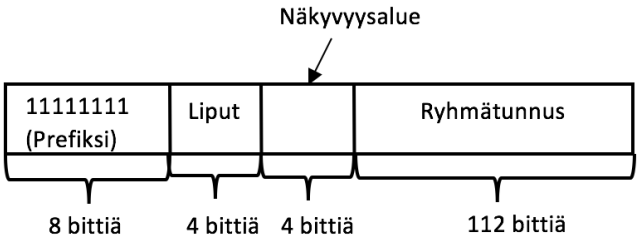
Kuva 3.6. *Site-local-osoitteen rakenne (perustuu lähteeseen: Deering & Hinden 2006, s. 11).*

Site-local-osoitteiden rakenne muodostuu omasta prefiksistä, aliverkon tunnisteesta ja liitännän tunnisteesta. Prefiksi heksamuotoon muutettuna saa muodon FEC0::/10. IPv6:n site-local-osoitteet vastaavat pitkälti IPv4:n privaatteja verkko-osoitteita. (Brown 2002, s. 133-135; Deering & Hinden 2006) Verkkolaitteiden hallinnan ja valvonnan toteuttamisen kannalta juuri globaalit unicast ja link-local-osoitteet ovat merkittävässä asemassa. Globaaleilla IPv6-osoitteilla voidaan määrittää laitteille globaalisti reititettävät hallintaosoitteet, joihin voidaan esimerkiksi ottaa yhteys etähallintaan tarkoitetuilla Telnet- ja SSH-protokollilla.

3.3 Multicast- ja anycast-osoitteet

Unicast-osoitteiden lisäksi IPv6-protokollassa on määritelty kaksi muuta pääosoitetyyppiä, joiden tarkoituksena on identifioida useampi kohde yksittäisellä osoitteella. Multicast-osoitteet identifioivat ryhmän liitäntöjä yhdellä osoitteella, jolloin multicast-osoitteeseen lähetetty paketti välitetään kaikkiin niihin verkon laitteiden liitäntöihin, jotka kuuluvat tämän osoitteen määrittelemään ryhmään. Jokainen liitäntä voi kuulua useampaan multicast-ryhmään tarkoittaen sitä, että paketit voidaan välittää tiettyyn liitäntään useammalla eri multicast-osoitteella. Toisin kuin IPv4-protokollassa, IPv6 ei tue enää yleislähetyksinä tunnettuja broadcast-osoitteita, vaan nämä on korvattu IPv6:n multicast-osoitteilla. Multicast-osoitteet voidaan tunnistaa ja erottaa unicast-osoitteista osoiteformaatin perusteella.

Kuvassa 3.7 on esitetty IPv6-protokollan multicast-osoitteen rakenne.



Kuva 3.7. *IPv6-protokollan multicast-osoitteen rakenne (perustuu lähteeseen: Deering & Hinden 2006, s. 13)*

Multicast-osoitteiden ensimmäisen tavun kaikki bitit ovat ykkösiä, jolloin multicast-osoitteet voidaan tunnistaa heksamuotoisesta prefiksistä FF00::/8. Lisäksi jokaisella multicast-osoitteella on näkyvyysalue (scope), joka rajoittaa sen alueen, jolle tietyn multicast-ryhmän liikenne on tarkoitettu. Tätä voidaan verrata IPv4-osoitteiden TTL-kenttään (Time To Live), joka IPv4:n kohdalla määrittelee multicast-pakettien ”elinaikaa” eli paketin mahdollisten hyppyjen lukumäärän. Esimerkiksi näkyvyysalue arvolla kaksi määrittelee paikallisen näkyvyysalueen (Link-Local scope), joka rajoittaa multicast-alueeksi reitittimien rajaaman alueen. Osoiterakenteessa oleva ryhmätunnus määrittelee ryhmän, johon multicast-osoite kuuluu. IPv6-protokollassa on ennalta määritelty useampia multicast-osoitteiden ryhmiä, joista tunnuksen arvolla yksi ja kaksi ovat merkittävimpiä verkkolaitteiden hallinnan kannalta. Ryhmätunnuksen arvolla yksi ja scope-arvolla kaksi muodostettu multicast-osoite FF02::1 (all-nodes multicast group) määrittää kaikki IPv6-solmut link-local-osoitteiden rajaamalla alueella. Vastaavasti ryhmätunnuksen arvolla kaksi ja scope-arvolla kaksi muodostettu multicast-osoite FF02::2 (all routers multicast group) määrittää kaikki reitittimet link-local-osoitteiden rajaamalla alueella. Kolmas erityinen multicast-osoitetyyppi on niin sanottu Solicited-node-osoite, jota verkkolaitteet käyttävät unicast-osoitteiden alustuksen yhteydessä. Solicited-node-osoite on muotoa FF02:0:0:0:0:1:FFxx:xxxx:, jossa prefiksin jälkeiset x-kirjaimet ovat verkkolaitteen 64-bittisen liitäntätunnisteen 24 vähiten merkitsevää bittiä. (Huitema 2000, s. 60-62; Deering & Hinden 2006)

Kuvassa 3.8 on esitetty otos reitittimen konfiguraatiosta, kun laitteen hallintaliitännässä on sallittu IPv6-protokolla sekä siihen on konfiguroitu IPv6-osoite. Kuvasta nähdään kaikki liitännän IPv6-osoitteet, jotka sille on joko konfiguroitu tai laite on itse määrittänyt. Kuva on hyvä osoitus siitä, kuinka yksittäisellä IPv6-liitännällä voi samanaikaisesti olla useita IPv6-osoitteita, joilla jokaisella on omat tehtävänsä IPv6-protokollan toiminnan kannalta.

```
FastEthernet0/1.777 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::213:C3FF:FEC2:AA2B
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:2060:BFFD:BFFD:213:C3FF:FEC2:AA2B, subnet is 2001:2060:BFFD:BFFD::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FFC2:AA2B
```

Kuva 3.8. *Reitittimen erään liitännän IPv6-osoitteistus hallintaosoitteen konfiguroinnin jälkeen.*

Kuvasta huomataan, että liitännällä on link-local-osoite FE80::213:C3FF:FEC2:AA2B, joka on muodostettu liitännän 48-bittisestä MAC-osoitteesta. Lisäksi huomataan, että hallintaliitännällä on globaali unicast-osoite 2001:2060:BFFD:BFFD:213:C3FF:FEC2:AA2B, joka kuuluu aliverkkoon 2001:2060:BFFD:BFFD::/64. Näiden lisäksi hallintaliitäntä on liittynyt kolmeen eri multicast-osoiteryhmään FF02::1, FF02::2 ja FF02::1:FFC2:AA2B. Ryhmistä ensimmäinen on siis kaikki IPv6-laitteet määrittävä ryhmä link-local-osoitteiden määrittämällä alueella. Koska kuvan laite on reititin, on sen hallintaliitäntä liittynyt lisäksi link-local-osoitteiden rajaaman alueen kaikki reitittimet määrittävään ryhmään. Kolmas liitännällä oleva multicast-osoite on Solicited-node-osoite, joka on muodostettu prefiksistä sekä 24:stä vähiten merkittävästä liitäntätunnisteen bitistä.

Kolmas IPv6-pääosoitetyypeistä anycast määrittelee myös ryhmän liitäntöjä, mutta hieman eri tavalla kuin multicat-osoitteet. Ero näiden kahden osoitetyypin välillä on havaittavissa siinä, kuinka paketit välitetään. Kun multicast-osoitteeseen lähetetty paketti välittyy kaikille sen ryhmään kuuluville liitännöille, anycast-osoitteeseen lähetetty paketti vastaavasti välittyy ainoastaan yhdelle tähän ryhmään kuuluvista liitännöistä. Lähetetty paketti välitetään ”lähimmälle” kohteelle, joka määritellään reititysprotokollien etäisyysmittauksilla. (Deering & Hinden 2006) Anycast-osoitteet eivät ole verkkolaitteiden hallinnan kannalta niin tärkeitä, joten niitä ei käsitellä tässä työssä tarkemmin.

3.4 ICMPv6

IPv6-protokollaa varten on määritelty uudempi versio myös ICMP-kontrolliprotokollasta (Internet Control Message Protocol) eli ICMPv6 (Internet Control Message Protocol version 6). IPv6-protokollaa tukevat laitteet hyödyntävät ICMPv6-protokollaa lähes vastaavalla tavalla kuin IPv4-protokollassa hyödynnetään sen tukemaan ICMPv4-protokollaa (Internet Control Message Protocol version 4), eikä sen toiminta siten eroa juurikaan alkuperäisestä ICMP-protokollasta. Joitakin muutoksia protokollan toteutukseen on tehty, joilla on merkittävä vaikutus IPv6-protokollan toimintaan. Samoin kuin IPv6-protokollaa myös ICMPv6-protokollaa on pyritty keventämään aikaisempaan ICMP-protokollaan

verrattuna poistamalla osa toiminnoista, joita ei katsottu enää tarpeellisiksi. Lisäksi protokollaan on yhdistetty toimintoja kolmesta eri IPv4-arkkitehtuuriin kuuluvasta protokollasta. Muun muassa IPv4:n ICMPv4-, IGMP- (Internet Group Membership Protocol) ja ARP-protokollat (Address Resolution Protocol) on yhdistetty osaksi ICMPv6-protokollan toteutusta. (Brown 2002, s. 68-69; Conta & Deering 2006)

IPv6-protokollaa tukevat laitteet käyttävät ICMPv6-protokollaa edelleen esimerkiksi raportoidakseen IP-pakettien prosessointivirheistä tai kun halutaan diagnosoida verkon tilaa ping-työkalun avulla aivan kuten IPv4-protokollassa. ICMPv6-protokollaa voidaan siis edelleen käyttää vastaavalla tavalla verkonhallinnan näkökulmasta verkkolaitteiden ja verkon tilan analysointiin ping- ja traceroute-työkalujen avulla. Näiden lisäksi ICMPv6 on oleellinen osa IPv6:n uusia keskeisiä ominaisuuksia kuten ND-protokollaa sekä autokonfigurointia ja siten kaikkien IPv6-protokollaa käyttävien laitteiden on tuettava myös uutta kontrolliprotokollaa. (Conta & Deering 2006)

3.5 ND-protokolla

NDP eli ND-protokolla on naapurisolmujen havaitsemiseen tarkoitettu protokolla, joka on keskeisessä osassa IPv6-protokollakokonaisuutta. Se tarjoaa IPv6-protokollaan useita uusia ominaisuuksia ja etuja, jotka eivät ole mahdollisia IPv4-protokollan kanssa. Tämän lisäksi se integroi useita IPv4-protokollan ominaisuuksia ja toimintoja, kuten ARP- ja RARP-protokollat (Reverse Address Resolution Protocol), reitittimien havaitsemisen sekä uudelleenohjaustoiminnot. Protokollan tavoitteena on ratkaista erilaisia naapurisolmujen väliseen vuorovaikutukseen liittyviä haasteita. Sen avulla verkon solmut voivat mainostaa verkon muille solmuille omaa olemassaoloaan sekä samalla saada tietoa verkon muista solmuista.

Taulukossa 3.1 on esitetty tärkeimmät ND-protokollan perustoiminnot ja -palvelut, jotka ovat käytössä yhdessä IPv6-protokollan kanssa.

Taulukko 3.1. *ND-protokollan perustoiminnot (Mun & Lee 2005, s. 51-60; Narten et al. 2007).*

Toiminto/palvelu	**Kuvaus**
Reitittimien havaitseminen (Router Discovery)	Menetelmä, jonka avulla verkon laitteet pyrkivät löytämään verkon reitittimet.
Verkkoprefiksien löytäminen (Prefix Discovery)	Kuinka verkon laitteet saavat selville ne kohdeosoitteet, jotka sijaitsevat samassa lähiverkossa ja mitkä vastaavasti reitittimen takana.

Verkkoparametrin löytäminen (Parameter Discovery)	Kuinka verkon laitteet saavat selville linkkien parametrit kuten esimerkiksi MTU-arvot (Maximum Transmission Unit) tai verkon parametrit kuten lähtevien pakettien eliniät.
Osoitteiden autokonfigurointi (Address Autoconfiguration)	Määrittelee mekanismin, jonka avulla verkon laitteet voivat automaattisesti määrittää tietylle liitännälleen yksilöidyn IPv6-osoitteen. Ns. tilaton autokonfiguraatio.
Osoitteiden selvittäminen (Address Resolution)	Määrittelee, kuinka verkon laitteet saavat selville naapurilaitteiden siirtokerroksen osoitteet pelkästään kohteen IP-osoitteen avulla.
Seuraavan hypyn määrittäminen (Next-hop Determination)	Algoritmi, jonka avulla voidaan selvittää, mille naapurilaitteelle paketti on lähetettävä, kun se halutaan välittää kohteen ilmaisemaan IP-osoitteeseen. Seuraava hyppy voi olla reititin tai paketin lopullinen kohde.
Saavuttamattoman naapurin havaitseminen (Neighbor Unreachability Detection)	Määrittää, kuinka laitteet havaitsevat, ettei naapurilaite ole enää saavutettavissa. Mahdollistaa uuden oletusreitin määrittämisen.
Duplikaattiosoitteiden havaitseminen (Duplicate Address Detection)	Kuinka laitteet voivat tarkistaa, ettei osoite, jota se on aikomassa käyttää ole jo jonkun toisen laitteen käytössä.
Uudelleenohjaus (Redirect)	Määrittää, kuinka reititin voi informoida verkon laitteita paremmasta seuraavasta hypystä, jota kautta voidaan saavuttaa tietty kohde.

Uusina ominaisuuksina IPv4-protokollaan verrattuna ND-protokolla yhdessä IPv6-protokollan kanssa mahdollistaa verkkoparametrien selvittämisen, IP-osoitteiden autokonfiguroinnin, seuraavan hypyn määrittämisen sekä saavuttamattoman naapurin ja duplikaattiosoitteiden havaitsemisen. (Mun & Lee 2005, s. 51-60)

ND-protokollassa on määritelty viisi erilaista viestityyppiä, jotka ovat RS (Router Solicitation), RA (Router Advertisement), NS (Neighbor Solicitation), NA (Neighbor Advertisement) sekä uudelleenohjaus- eli Redirect-viestit. Kaikki ND-protokollan viestit välitetään ICMPv6-paketteina. (Mun & Lee 2005, s. 51-60)

Taulukossa 3.2 on esitetty kaikki ND-protokollassa määritetyt viestityypit sekä niiden käyttötarkoitukset.

Taulukko 3.2. *ND-protokollan viestityypit (Mun & Lee 2005, s. 60-67; Narten et al. 2007).*

Viestityyppi	**Kuvaus**
Router Solicitation (RS)	Solmut käyttävät havaitakseen verkon reitittimet. Kun verkon solmun liitäntä aktivoituu, voi solmu lähettää RS-viestin, jolla se voi pyytää reitittimiä lähettämään välittömästi RA-viestin ilman, että solmun tarvitsee odottaa seuraavaa reitittimeltä lähetettävää RA-viestiä.
Router Advertisement (RA)	Reitittimet voivat mainostaa olemassaoloaan lähettämällä RA-viestejä säännöllisesti tai vastaamalla solmuilta lähetettyihin RS-viesteihin. RA-viestit sisältävät muun muassa prefiksitietoja, joiden avulla solmut voivat generoida itselleen IP-osoitteen.
Neighbor Solicitation (NS)	Kun solmu linkitetään muiden solmujen kanssa, tarkistaa se ensin, ettei verkossa muilla olevilla solmuilla ole duplikaattiosoitteita. NS-viestien avulla solmut voivat lisäksi selvittää naapurisolmujen siirtokerroksen osoitteet sekä tarkistaa muiden solmujen saatavuuden.
Neighbor Advertisement (NA)	Solmut lähettävät NA-viestejä vastauksina toisilta solmuilta lähetettyihin NS-viesteihin. Viestejä käytetään lisäksi muun muassa ilmaisemaan solmun siirtokerroksen osoitteiden muutoksista.
Redirect	Uudelleenohjausviestejä käytetään informoimaan päätelaitetta paremmasta ensimmäisestä hypystä, joka johtaa tiettyyn kohdeosoitteeseen.

Verkonhallinnan näkökulmasta ND-protokollan tarjoamista ominaisuuksista oleellisimpia ovat siirtokerroksen osoitteiden selvittäminen, osoitteiden autokonfiguraatio sekä duplikaattiosoitteiden havaitseminen.

3.5.1 Siirtokerroksen osoitteiden selvittäminen

Koska ARP-protokollaa ja broadcast-osoitteita ei enää käytetä IPv6-protokollan kanssa, tulee verkon solmujen pystyä selvittämään naapurisolmujen siirtokerroksen osoitteet eli MAC-osoitteet muulla tavalla. Yksi ND-protokollan toiminnoista on mahdollistaa siirtokerroksen osoitteiden selvittäminen ICMPv6-viestien ja broadcast-osoitteet korvanneiden multicast-osoitteiden avulla. Toisin sanoen ARP-protokollan toiminnot IPv6-protokollan tapauksessa on korvattu ICMPv6-viestein suoritetulla prosessilla, jossa solmu tiedustelee näiden viestien avulla naapurisolmulta tämän siirtokerroksen osoitetta. Tällä prosessilla saavutetaan sama lopputulos kuin ARP-protokollalla IPv4:n yhteydessä. (Mun & Lee 2005, s. 56-59; Narten et al. 2007)

Solmulla voi olla tiedossa naapurisolmun paikallisen linkin unicast-osoite, mutta ei tätä vastaavaa siirtokerroksen osoitetta. Tällöin unicast-tyyppisen paketin välittäminen naapurisolmulle ei onnistu ennen kuin paketin lähettävä solmu saa selville ND-protokollassa määriteltyjen viestien avulla naapurisolmun paikallisen linkin liitännän siirtokerroksen osoitteen. Tämä prosessi perustuu ICMPv6-tyyppisten Neighbor Solicitation ja Neighbor Advertisement -viestien välittämiseen naapurisolmujen välillä. Ensin pyynnön lähettävä solmu luo välimuistiinsa pyydettyä osoitetta varten kirjauksen, johon saatu osoite lopulta kirjataan ja josta se on myöhemmillä kerroilla luettavissa. Tämän jälkeen tiedusteleva solmu lähettää naapurisolmulle Neighbor Solicitation -viestin käyttäen erityistä vastaanottavan solmun multicast-osoitetta eli niin sanottua Solicited-node-osoitetta. Kun solmupiste vastaanottaa lähetetyn Neighbor Solicitation -viestin, tarkastaa se viestin oikeellisuuden ja luo omaan välimuistiinsa vastaavanlaisen kirjauksen naapurisolmun osoitetta varten tai vastaavasti päivittää oman välimuistinsa kirjauksen tämän naapurin osalta. Lopuksi solmu lähettää naapurilleen takaisin Neighbor Advertisement -viestin sisältäen kyselyn kohteena olevan solmun liitännän siirtokerroksen osoitteen. Nyt alkuperäisen Neighbor Solicitation -viestin lähettänyt solmu voi päivittää oman välimuistinsa tämän osoitteen osalta, ja alkuperäinen unicast-paketti voidaan välittää naapurisolmulle käyttäen paikallisen linkin siirtokerroksen osoitetta, joka tämän prosessin avulla on saatu selville. (Mun & Lee 2005, s. 56-59; Narten et al. 2007)

3.5.2 Unicast-osoitteiden tilaton autokonfigurointi

Thomson et. al. (2007) ovat määritelleet IPv6-protokollan tilattoman autokonfiguraation RFC-dokumentissa 4862. Siinä on määritelty tarkemmin tässä ja seuraavassa alaluvussa käsiteltävät tilaton autokonfiguraatio ja duplikaattiosoitteiden tarkistus. IPv6-protokolla tarjoaa mahdollisuuden tätä IP-protokollaversiota tukevien verkkolaitteiden generoida itselleen automaattisesti IPv6-osoitteet. Protokollassa on määritelty kaksi automaattisen

konfiguroinnin tapaa, tilaton ja tilallinen autokonfigurointi. Tilallisella autokonfiguraatiolla tarkoitetaan vastaavaa prosessia kuin IPv4-protokollassa, jossa laitteet lähettävät kyselyn DHCP-palvelimelle (Dynamic Host Configuration Protocol) saadakseen IP-osoitteen. Tässä työssä ei käsitellä tilallista autokonfiguraatioita, vaan keskitytään ainoastaan tilattomaan autokonfiguraatioon ja siihen, kuinka sitä voidaan hyödyntää verkkolaitteiden hallintaosoitteiden muodostamiseen.

Tilattoman autokonfiguraation ideana on, että IPv6-protokollaa tukevat laitteet voivat generoida itselleen yksilöidyn osoitteen ilman erillisiä palvelimia. Käytännössä tämä tapahtuu reitittimien avulla, joilla mahdollistetaan muiden verkkolaitteiden generoida itselleen IPv6-osoite hyödyntämällä reitittimiltä saatua informaatiota. Tällöin jokainen verkkolaite voi muodostaa itselleen osoitteen hyödyntämällä omaa paikallista tietoaan verkosta sekä reitittimien mainostamaa prefiksitietoa. Yleisesti tilaton autokonfiguraatio käsittää kolme erillistä vaihetta. Ensimmäisessä vaiheessa liitännälle muodostetaan paikalliseen käyttöön tarkoitettu link-local-osoite, jonka jälkeen liitännälle voidaan generoida globaalisti uniikki unicast-osoite. Oleellisena osana tilattomaan autokonfiguraatioon ja siten edellä mainittujen osoitteiden muodostamiseen liittyy osoitteiden duplikaattitarkistus, jonka tarkoituksena on varmistaa, ettei liitännälle luodut osoitteet ole jo käytössä jollakin toisella laitteella samassa aliverkossa. (Thomson et al. 2007)

Tilatonta autokonfiguraatiota voidaan siis osaltaan hyödyntää myös verkkolaitteiden hallinta- ja valvontayhteyksien toteuttamiseen. Automatisoidun osoitteenmuodostuksen hyöty tulee esille siinä, ettei lähiverkon verkkolaitteille välttämättä tarvitse manuaalisesti konfiguroida hallintaosoitteita, mikäli verkossa on reitittävä laite, jonka avulla muissa verkkolaitteissa voidaan hyödyntää autokonfigurointia. Tällöin laitteet voivat generoida itselleen yksilöidyn hallintaliitännän IPv6-osoitteen riippumatta siitä, missä hallintaverkossa laite sijaitsee. Näin periaatteessa jokainen etähallinnassa oleva verkkolaite voidaan siirtää haluttuun toiseen hallintaverkkoon ilman, että laitteelle tulee manuaalisesti vaihtaa hallintaosoitetta, vaan laite saa uudessa verkossa autokonfiguraation ansiosta uuden osoitteen paikallisesta hallintaverkosta. Tämän jälkeen laitteen automaattisesti konfiguroidun hallintaosoitteen kautta laitteelle voidaan heti muodostaa uusi etäyhteys olettaen, että muut verkkotekniset asiat, kuten reititys ovat kunnossa. Ilman reitittimiä muut verkkolaitteet, kuten esimerkiksi kytkimet eivät pysty generoimaan itselleen globaalia hallintaosoitetta, vaan ainoastaan paikalliseen käyttöön tarkoitetun link-local-osoitteen. Tällöin globaali hallintaosoite tulee konfiguroida liitännälle manuaalisesti. (Thomson et al. 2007)

Kun verkkolaitteen liitäntä aktivoituu ja liitännässä sallitaan IPv6-operaatiot, luo laite liitäntään automaattisesti paikalliseen käyttöön tarkoitetun link-local-osoitteen, joka protokollan määritelmän mukaan tulee siis vähintään olla jokaisella aktiivisella IPv6-protokollaa tukevalla liitännällä. Ennen kuin tätä osoitetta voidaan käyttää ja automaattisen konfiguroinnin prosessia jatkaa, tulee osoite vielä tarkastaa protokollan määritysten mukaan mahdollisten duplikaattiosoitteiden varalta. Duplikaattiosoitteiden havaitseminen on osa ND-protokollan ominaisuuksia ja sitä käsitellään tarkemmin seuraavassa alaluvussa.

Koska laitteiden liitäntätunnukset ovat lähes poikkeuksetta globaalisti uniikkeja, on link-local-osoitteiden duplikaattitarkistus yleensä negatiivinen. Muutoin link-local-osoite tulisi konfiguroida manuaalisesti, mikä estäisi autokonfiguraatioprosessin jatkumisen. Kun duplikaattiosoitteiden tarkistus on suoritettu, eikä muodostetusta link-local-osoitteesta löydetty verkosta duplikaatteja, tulee verkkolaitteen löytää naapurireitittimet, jotka voisivat mainostaa verkkolaitteelle globaalin unicast-osoitteen muodostusta varten verkkoprefiksin. Tässä kohtaa verkkolaiteella on IP-tason yhteys sen naapurilaitteille juuri luodun link-local-osoitteen ansiosta. Link-local-osoitteen muodostuksen yhteydessä liitäntä liittyy osaksi tiettyjä multicast-ryhmiä. Olennaisin näistä on kaikki verkkolaitteet määrittelevä All-node multicast -osoite FF02::1, joka mahdollistaa reitittimien lähettämien NA-viestien saapumisen verkkolaitteille. Lisäksi liitännälle tulee märittää alustavan link-local-osoitteen pohjalta Solicited-node-osoite, joka mahdollistaa NS-viestien lähettämisen verkkolaitteelta esimerkiksi osoitteiden duplikaattitarkastuksen yhteydessä. (Narten 1999; Thomson et al. 2007)

Globaali unicast-osoite muodostetaan lisäämällä liitäntätunnuksen eteen reitittimen mainostama tietynpituinen prefiksi, jolloin osoite saadaan lopulliseen 128-bittiseen muotoon. Verkkolaitteet saavat prefiksitiedot reitittimien mainostamissa RA-viesteissä, joita ne mainostavat All-nodes multicast -osoitteeseen ennalta määritetyin väliajoin. Koska reitittimien lähettämien RA-viestien lähetysvälit voivat vaihdella sekunneista useisiin kymmeniin minuutteihin, on tärkeää, että juuri verkkoon liitetyt verkkolaitteet saavat osoitteensa mahdollisimman nopeasti ilman, että joutuvat odottamaan pitkän ajan ennen kuin seuraava RA-viesti saapuu reitittimeltä. Tästä syystä verkkolaitteet voivat lähettää yhden tai useamman RS-viestin saadakseen globaalin unicast-osoitteen sen jälkeen kuin niiden liitännälle on muodostettu uniikki link-local-osoite. Näitä osoitteita verkkolaitteet käyttävät lähdeosoitteina lähettäessään RS-viestejä reitittimille. Mikäli verkossa on reitittimiä, vastaavat ne näihin viesteihin välittömästi, jolloin verkkolaitteiden ei tarvitse odottaa seuraavan säännöllisesti lähetettävän RA-viestin saapumista. Kun verkkolaite on generoinut globaalin unicast-osoitteen reitittimeltä saapuneen RA-viestin sisällöstä löytyneen prefiksitiedon sekä liitäntätunnuksen avulla, tarkastetaan muodostettu osoite link-local-osoitteiden tapaan yleensä vielä duplikaattiosoitteiden varalta. Tilattomaan autokonfiguraatioon liittyvät prosessit voidaan yleensä suorittaa rinnakkain, jolloin koko prosessiin kuluvaa aikaa saadaan vähennettyä. Esimerkiksi liitännälle luodun link-local-osoitteen duplikaattitarkastus voidaan suorittaa samanaikaisesti, kun odotetaan RA-viestin saapumista liitäntään, johon laite on luomassa globaalia unicast-osoitetta. Näin voidaan vähentää selvästi koko prosessiin kuluvaa aikaa, jolloin ei tarvitse odottaa, että edellinen prosessi on saatu suoritettua loppuun. (Narten 1999; Thomson et al. 2007)

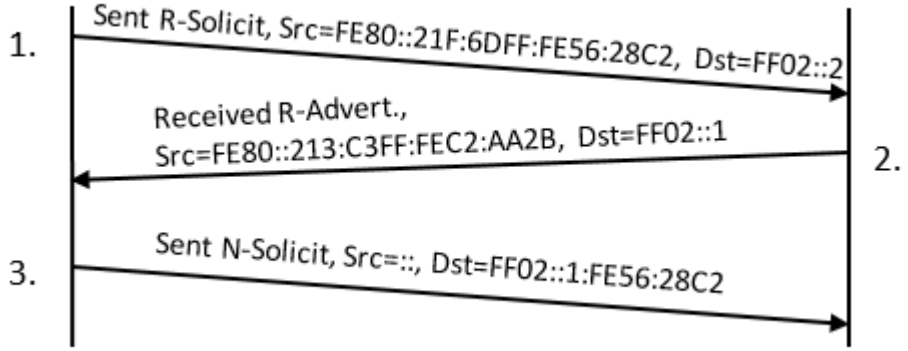
3.5.3 DAD - Duplikaattiosoitteiden havaitseminen

Kun verkkolaitteen liitännälle ollaan määrittämässä joko link-local-osoitetta tai globaalia unicast-osoitetta, voidaan ND-protokollan osana toteutetun DAD-algoritmin (Duplicate

Address Detection) avulla havaita, onko laitteelle asetettu unicast-osoite jo jonkun toisen verkkolaitteen käytössä. Mikäli unicast-osoitteen määrityksen jälkeen menetelmä havaitsee verkosta duplikaattiosoitteen, ei kyseistä osoitetta voida siten käyttää liitännän osoitteena, vaan liitännälle tulee määrittää uusi unicast-osoite. Thomson et. al. (2007) ovat määritelleet RFC-dokumentissa 4862, että jokaisen liitännän unicast-osoitteen ainutlaatuisuus pitäisi tarkastaa algoritmin avulla. Globaalien unicast-osoitteiden duplikaattitarkistus verkkolaitteen liitännöissä voidaan kuitenkin konfiguroimalla estää tietyissä tilanteissa, mutta tällaista protokollan optimointia ei kuitenkaan suositella. Algoritmi ei itsessään ota kantaa siihen, kuinka unicast-osoite liitännälle on asetettu eli, onko osoitteen asettaminen seurausta automaattisesta konfiguroinnista, DHCPv6- protokollan (Dynamic Host Configuration Protocol version 6) käytöstä vai osoitteen manuaalisesta konfiguroinnista. Kaikissa tilanteissa osoitteiden ainutlaatuisuus tulisi tarkistaa ND-protokollan mahdollistamalla DAD-algoritmilla.

Duplikaattiosoitteiden havaitseminen on siis osa ND-protokollan toteutusta ja algoritmi käyttääkin ND-protokollassa määriteltyjä Neighbor Solicitation ja Neighbor Advertisement-viestejä. Kun verkkolaitteen liitäntä on saanut uuden unicast-osoitteen, on osoite vielä niin sanotusti alustava (tentative) osoite. Alustavan osoitteen saaneen liitännän tulee ottaa vastaa NS- ja NA-viestejä, joissa tämä alustava osoite on kohdeosoitteena, mutta hylätä vielä muut paketit. Toisin sanoen osoitteen alustus on vielä kesken, eikä liitäntä voi alustavalla osoitteella osallistua vielä varsinaiseen liikennöintiin. Ennen kuin solmu voi lähettää NS-viestin selvittääkseen duplikaattiosoitteiden olemassaolon, tulee liitännän liittyä kaikki laitteet määrittämään multicast-osoitteiden ryhmään, jotta NS-viestit saadaan välitettyä liitäntään, jonka varalta duplikaattiosoitteen olemassaolo halutaan tarkastaa. Verkkolaitteet lähettävät NS-viestin, jonka kohdeosoitteeksi on asetettu tarkastettava unicast-osoite multicast-osoitteeksi muutettuna. (Thomson et al. 2007)

Alla olevassa kaaviokuvassa 3.9 on esitetty havainnollistus tilattomasta autokonfiguraatiosta ja sitä seuranneen duplikaattiosoitteen tarkistusprosesseista. Kuvan tilanteessa luodaan globaali unicast-osoite verkkolaitteen liitäntään ja sen ainutlaatuisuus tarkistetaan DAD-algoritmilla. Kuvassa esitettävät tiedot ja osoitteet on otettu suoraan erään Ciscon valmistaman laboratoriolaitteen lokitiedoista, kun on testattu IPv6-osoitteen määrittämistä laitteelle tilattomalla autokonfiguraatiolla.



Kuva 3.9. *Havainnollistus globaalin unicast-osoitteen muodostamisesta tilattomalla autokonfiguraatiolla ja tämän osoitteen duplikaattitarkastuksesta.*

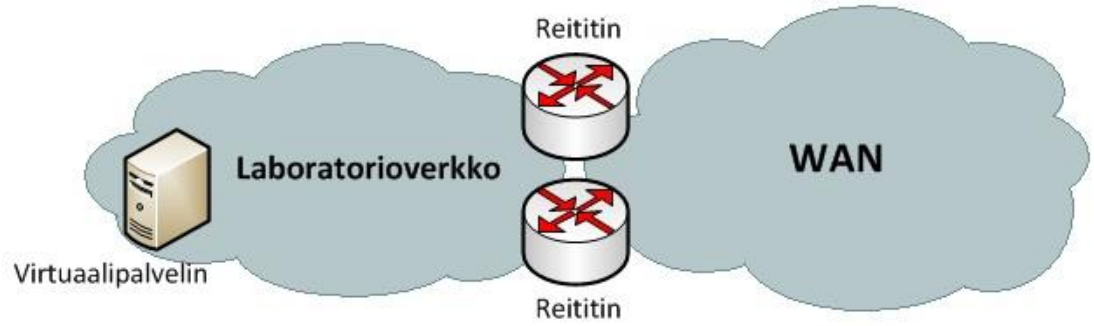
Kuvassa vasen puoli esittää kytkintä, jonka verkkoliitäntään ollaan määrittämässä globaalia unicast-osoitetta tilattomalla autokonfiguraatiolla. Vastaavasti oikealla puolella on reititin, jonne kytkimeltä lähetettävät viestit saapuvat. Kuvassa ensimmäinen nuoli ilmaisee tilattoman autokonfiguraation ensimmäistä tapahtumaa, jossa kytkin lähettää RS-viestin kohdeosoitteella, joka määrittää multicast-alueen kaikki reitittimet. Tässä tapauksessa viestin lähdeosoitteena on liitännän link-local-osoite, joka on luotu liitännälle jo aiemmin myös laitteen suorittaman autokonfiguraation seurauksena. Tämän kytkimen lähettämän RS-viestin tarkoituksena on lähettää reitittimille pyyntö, jotta jokin verkon reitittimistä lähettäisi kytkimelle tiedon verkkoprefiksistä, joka tarvitaan globaalin unicast-osoitteen luomiseen. Kun RS-viesti on saapunut reitittimelle, esittää kuvan toinen nuoli seuraavaa tapahtumaa, jossa reititin vastaa tähän kytkimeltä lähetettyyn RS-viestin mukana tulleeseen pyyntöön. Kuvan tilanteessa kytkin vastaanottaa RA-viestin, jonka lähdeosoitteena on nyt viestin lähettävän reitittimen link-local-osoite ja vastaavasti kohdeosoitteena multicast-osoite, joka määrittää kaikki IPv6-verkkolaitteet link-local-osoitteiden alueella. Tämän viestin mukana kytkin vastaanottaa tiedon verkkoprefiksistä, jonka avulla se voi luoda itselleen globaalin IPv6-osoitteen tämän prefiksin ja kyseisen liitännän liitäntätunnuksen avulla. Kun kytkin on luonut itselleen globaalin unicast-osoitteen, tarkistaa laite vielä tämän osoitteen ainutlaatuisuuden. Kuvan kolmas tapahtuma kuvaa tilannetta, jossa kytkin lähettää osoitteen duplikaattitarkistusviestin Solicited-node-osoitteeseen käyttäen lähdeosoitteena erityistä nollaosoitetta ::/128, jota voidaan käyttää lähdeosoitteena unicast-osoitteiden alustuksessa, jolloin reitittimet tietävät olla reitittämättä IPv6-paketteja, joissa lähdeosoitteena on tällainen nollaosoite. Mikäli lähetettyyn viestiin ei tule NA-viestinä vastausta, ei unicast-osoitteelle ole löytynyt verkosta duplikaattia. Tällöin kyseinen osoite voidaan turvallisesti asettaa liitännälle ja tilattoman autokonfiguraation prosessi on suoritettu loppuun.

4. LABORATORIOVERKKO

Edellisissä luvuissa käsiteltiin verkkolaitteiden hallintaan ja valvontaan käytettäviä protokollia sekä IPv6-protokollaa yleisellä tasolla. Nämä luvut toimivat taustatietoina seuraaville luvuille, joissa hallinta- ja valvontatyökalujen sekä IPv6-protokollan yhteensopivuutta on tarkoitus tutkia erikseen suunnitellussa ja toteutetussa laboratorioympäristössä. Laboratorioympäristön tarkoitus on toimia yksinkertaisena, mutta todellisuutta mallintavana testausympäristönä, jossa tehtävien tutkimusten avulla voidaan tehdä päätelmiä verkkolaitteiden hallinnan ja valvonnan toimivuudesta IPv6-osoitteisessa ympäristössä. Aluksi luvussa esitellään laboratorioverkon topologia, laitteisto sekä verkossa sijaitsevan virtuaalipalvelimen toiminta ja rooli osana tehtäviä tutkimuksia. Seuraavaksi esitellään, kuinka IPv6-protokolla voidaan ottaa käyttöön laboratorioverkon laitteissa ja kuinka IPv6-hallintaosoitteet voidaan konfiguroida laitteisiin. Lopuksi esitellään vielä laboratorioverkon laitteiden IPv6-hallintaosoitteistus.

4.1 Topologia ja laitteisto

Kuvassa 4.1 on esitetty laboratorioverkon looginen topologia, josta nähdään, kuinka laboratorioverkko on yhteydessä operaattorin WAN-verkkoon (Wide Area Network). Looginen topologia esittää yksinkertaistettuna, kuinka eri verkot on yhdistetty loogisella tasolla toisiinsa.

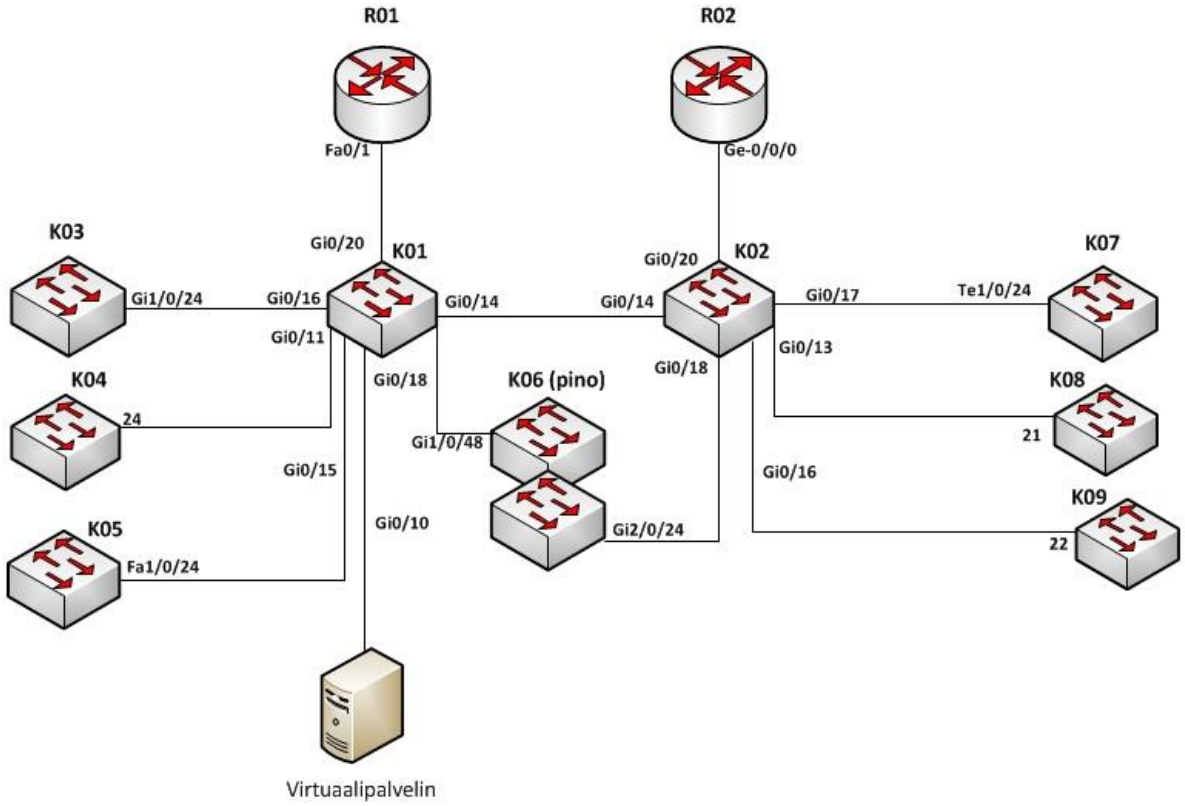


Kuva 4.1. *Laboratorioverkon looginen topologia.*

Kuvasta 4.1 havaitaan, että laboratorioverkko on yhdistetty operaattorin WAN-verkkoon verkon reunalla olevien kahden reitittimen kautta. Reitittimet vastaavat laboratorioverkon ja WAN-verkon välisen liikenteen reitityksestä ja mahdollistavat liikennöinnin laboratorioverkosta ulospäin.

Kuvassa 4.2 on esitetty laboratorioverkon fyysinen topologia, josta nähdään, kuinka laboratorioverkon laitteet on fyysisesti yhdistetty toisiinsa. Kuvassa on esitetty eri verkko-

laitteiden välille muodostetut linkit yhdessä niiden porttinumeroiden kanssa, joihin laitteiden väliset kaapelit on fyysisesti kytketty. Verkkoon sijoitetut verkkolaitteet koostuvat eri laitevalmistajien pääosin erimallisista laitteista. Laaja laitekanta mahdollistaa monipuolisen tutkimusympäristön laajentaen näin tutkimusta eri laitevalmistajien laitteiden välille, mutta myös saman laitevalmistajan eri laitemallien välille. Verkkoon sijoitetut laitteet koostuvat tiettyjen laitevalmistajien niistä laitemalleista, joita on tällä hetkellä runsaasti käytössä organisaatioiden lähiverkoissa.



Kuva 4.2. *Laboratorioverkon fyysinen topologia.*

Kuvasta 4.2 nähdään, että laboratorioverkkoon sijoitetut reitittimet siis toimivat verkon reunalla ohjaten liikenteen verkkoon sisään ja verkosta ulospäin. Laboratorioverkon reitittimet koostuvat kahden eri laitevalmistajan reitittimistä. Kuvassa vasemmanpuoleinen reititin R01 on Ciscon valmistama ja vastaavasti oikeanpuoleinen R02 on Juniperin valmistama reititin. Laboratorioverkossa sijaitsevien reitittimien perään on kytketty useita kytkimiä, joiden avulla tutkimukset voidaan suorittaa laajemmin useiden erimallisten verkkolaitteiden välillä. Kaikki verkkoon sijoitetut kytkimet ovat joko HP:n (Hewlett-Packard) tai Ciscon valmistamia. Suoraan R01:n perään portista Fa0/1 (Fast Ethernet) on kytketty Ciscon runkokytkin K01 sen porttiin Gi0/20 (Gigabit Ethernet). Tässä merkintä Fa0/x tarkoittaa reitittimen Fast Ethernet -tyyppistä fyysistä porttia, jossa kirjain x ilmaisee reitittimen fyysisen LAN-portin numeron (Cisco 2013). Vastaavasti Ciscon kytkimen merkintä Giy/z tarkoittaa Gigabit Ethernet -tyyppistä kytkimen porttia, jossa kirjain y tarkoittaa kytkimen moduulin numeroa ja kirjain x kytkimen fyysisen liitäntäportin numeroa

(Cisco 2016a). Reitittimen R02:n perään sen portista Ge-0/0/0 (Gigabit Ethernet) on kytketty toinen vastaavanlainen Ciscon kytkin K02 kuin on K01. Tässä merkintä Ge-x/y/z tarkoittaa Juniperin tapaa kuvata sen reitittimien Gigabit Ethernet -tyyppisiä portteja, jossa kirjain x ilmaisee reitittimen moduulipaikan, y ilmaisee fyysisen liitäntämoduulin PIM (Physical Interface Module) ja kirjain z ilmaisee fyysisen portin reitittimen liitäntämoduulissa (Juniper 2012). Kuvasta huomataan, että kytkimet K01 ja K02 ovat lisäksi kytketty toisiinsa molempien porteista Gi0/14. Kytkimen K01 perään portista Gi0/16 on kytketty Ciscon kytkin K03. Kuvassa kytkimen K03 porttinumerossa Gi1/0/24 ensimmäinen luku tarkoittaa mahdollisen kytkinpinon järjestyslukua (Cisco 2016a). Koska kuvan tilanteessa ei kyseessä ole pinokytkin, on porttinumerossa pinon järjestysluku yksi. Muut porttinumeron luvut muodostuvat samalla tavalla kuin aikaisemmin kytkimen K01 tapauksessa. Kytkimen K01 porttiin Gi0/11 on kytketty kytkin K04, joka on HP:n valmistama. HP:n kytkimien kohdalla porttinumerot on esitetty HP:n tapaan ainoastaan kytkimen fyysistä porttia kuvaavalla järjestysnumerolla, kuten kytkimen K04 kohdalla numerolla 24. Samaisen K01-kytkimen porttiin Gi0/15 on kytketty K05-kytkin. Lisäksi kytkimen K01 porttiin Gi0/10 on kytketty laboratorioverkkoon sijoitettu virtuaalipalvelin, jota käsitellään tarkemmin tämän alaluvun lopussa. Kytkimien K01 ja K02 porteista Gi0/18 on luotu linkit pinokytkimeen K06, joka muodostuu kahdesta Ciscon C3750-sarjan kytkimestä. Kuvasta nähdään, että kytkimestä K02 on tehty linkki pinokytkimen jäsenkytkimen porttiin Gi2/0/24. Nyt kytkimen porttinumerossa ensimmäinen luku kaksi ilmaisee, että kyseessä on pinon kakkoskytkin. Kytkimen K02 perään on kytketty lisäksi vielä kolme muuta kytkintä K07, K08 ja K09. Kytkimen K02 portista Gi0/17 on kytketty vielä yksi Ciscon valmistama kytkin K07 ja tämän porttiin Te1/0/24. Tässä merkinnässä kirjaimet Te (TenGigabit Ethernet) tarkoittavat TenGigabit Ethernet -tyyppistä porttia ja sen perässä olevat numerot x/y/z muodostavat porttinumeron samalla tavalla kuin kytkimen K03 tapauksessa (Cisco 2016d). K02:n perässä on lisäksi vielä kaksi HP:n kytkintä K08 ja K09, jotka on liitetty K02:n portteihin Gi0/13 ja Gi0/16.

Taulukossa 4.1 on esitetty tutkimusten kannalta olennaisimpia tietoja kaikista laboratorioverkkoon asennetuista verkkolaitteista.

Taulukko 4.1. *Laboratorioverkon laitteiden tunnukset, laitemallit ja ohjelmistoversiot.*

LAITETUNNUS	LAITEMALLI	OHJELMISTOVERSIO
R01	Cisco 1841	15.1(4)M10
R02	Juniper srx210	12.1.X46-D40.2
K01	WS-C2960G-24TC-L	12.2(55)SE10
K02	WS-C2960G-24TC-L	12.2(55)SE10
K03	WS-C2960S-24PS-L	12.2(55)SE10
K04	HP 2620-24 J9623A	RA.15.18.0008
K05	ME-C3750-24TE	12.2(58)SE2
K06 (STACK)	WS-C3750G-48TS / WS-C3750G-24TS-1U	12.2.(55)SE1 (molemmat kytkimet samalla ohjelmistoversiolla)
K07	WS-C3850-24XU	03.07.02E
K08	HP 2920-24G-PoE+ J9727A	WB.15.18.0007
K09	HP 2610-24 J9085A	R.11.22

Taulukossa vasemmassa sarakkeessa esitetyillä laitetunnuksilla viitataan jatkossa tutkimusten yhteydessä tutkittaviin laitteisiin. Keskimmäisessä sarakkeessa on esitetty jokaisen verkkolaitteen laitemalli ja oikeanpuoleisessa sarakkeessa verkkolaitteeseen asennetun ohjelmiston versionumero. Taulukossa esitetyillä ohjelmistoversioilla viitataan niihin laitteiden ohjelmistoversioihin, joilla tutkimukset on suoritettu.

Oleellisena osana laboratorioverkon rakennetta on kytkimen K01 perään yhdistetty virtuaalipalvelin, jonka tarkoituksena on tarjota ympäristö, josta verkkolaitteisiin muodostettavia hallinta- ja valvontayhteyksiä voidaan tutkia. Palvelimelle on asennettu Ubuntun virtuaalikone, joka on versioltaan Ubuntu 14.04.4 LTS. Palvelimelle asennettuun virtuaalikoneeseen on asennettu kaikki työssä tehtäviä tutkimuksia varten tarvittavat hallinta- ja valvontapalvelimet. Virtuaalikoneen tarkoituksena on mahdollistaa tutkittavien hallinta- ja valvontaprotokollien Telnetin, SSH:n sekä SNMP:n ajaminen verkkolaitteisiin. Lisäksi virtuaalikoneelle on asennettu yleiset verkonhallinnan aputyökalut, kuten ping ja traceroute sekä näiden IPv6-protokollaa tukevat versiot. Työkalujen avulla voidaan esimerkiksi ensin varmistaa verkkolaitteiden saavutettavuus, jonka jälkeen voidaan testata tarkemmin edellä mainittujen hallinta- ja valvontatyökalujen toimivuutta tutkittaviin verkkolaitteisiin. Virtuaalikoneelle on asetettu IPv6-osoite 2001:2060:BFFD:BFFD::3, jota käytetään lähdeosoitteena työn myöhemmässä vaiheessa tehtävissä tutkimuksissa.

4.2 IPv6-protokollan käyttöönotto verkkolaitteissa

Kaikissa laboratorioverkon laitteissa IPv6-protokolla ei ole suoraan käytettävissä, vaan osa laitteista vaatii erityisiä konfiguraatioita, jotta IPv6-operaatiot saadaan toimimaan niissä olettaen, että laitemalli ja laitteeseen asennettu ohjelmisto ovat IPv6-protokollaa tukevia. Lisäksi IPv6-operaatioiden konfigurointi esimerkiksi tietyssä VLAN-liitännässä vaatii hieman IPv4-protokollan vastaavista poikkeavia komentoja. Tässä ja seuraavassa alaluvussa käydään tarkemmin läpi, kuinka IPv6-protokolla voidaan ottaa käyttöön eri valmistajien verkkolaitteissa ja kuinka IPv6-hallintaosoitteet voidaan määritellä laboratorioverkossa oleville laitteille.

Ciscon 1841-sarjan reitittimessä IPv6-protokollan käyttöönotto vaatii, että se sallitaan globaalisti reitittimellä. Oletuksena IPv6-pakettien välitys reitittimen verkkoliitännöissä on siis estetty. Protokolla ja erityisesti IPv6-pakettien välitys voidaan sallia globaalisti reitittimellä kuvassa 4.3 esitetyllä konfiguraatiolla.

```
(config)#ipv6 unicast-routing
```

Kuva 4.3. *IPv6-protokollan salliminen ja globaali käyttöönotto reitittimessä R01.*

Edellä esitetty komento sallii IPv6-protokollan koko kytkimessä ja ilman tätä komentoa esimerkiksi liitäntöihin määritetyt IPv6-osoitteet eivät toimi, koska komennolla sallitaan reitittimen liitäntöjen välittää unicast-paketteja. Tällä komennolla saadaan sallittua myös ND-protokolla ja siten sen tuomat ominaisuudet, kuten tilaton autokonfiguraatio ja ARP-protokollaa vastaava IPv6-toiminnallisuus. Kun protokolla on sallittu reitittimellä globaalisti, voidaan sen liitännöille määrittää IPv6-osoitteet. (Brown 2002, s. 160-161; Desmeules 2003) Alaluvussa 4.3 käsitellään tarkemmin, kuinka laboratorioverkossa sijaitseviin eri laitevalmistajien reitittimiin ja kytkimiin voidaan konfiguroida tutkimuksia varten IPv6-hallintaosoitteet.

Juniperin srx210-sarjan reitittimessä ja sen Junos-käyttöjärjestelmässä IPv6-pakettien välitys on oletuksena estetty. Oletuskonfiguraatioissa IPv6-pakettien välitys reitittimellä on estetty (drop-tilassa), joten IPv6-pakettien välitys täytyy erikseen sallia reitittimen konfiguraatiossa. Tämä voidaan tehdä joko pakettikohtaisesti tai liikennevuohon perustuvasti. Pakettikohtainen IPv6-pakettien välitys tarkoittaa, että pakettien välitys tapahtuu tilattomasti, jolloin jokainen IPv6-paketti käsitellään yksittäin pakettikohtaisten ominaisuuksiensa perusteella. Vastaavasti vuoperusteisessa pakettien välityksessä pakettien välitys on tilallista, jolloin useita IPv6-paketteja käsitellään istuntokohtaisesti samalla tavalla. (Juniper 2013) Kuvassa 4.4 on esitetty, kuinka IPv6-pakettien välitys voidaan sallia Junos-käyttöjärjestelmää käyttävässä Juniperin reitittimessä.

```
              # set security forwarding-options family inet6 mode ?
Possible completions:
  drop                 Disable forwarding
  flow-based           Enable flow-based forwarding
  packet-based         Enable packet-based forwarding
              # set security forwarding-options family inet6 mode packet-based
              # exit
              > show security flow status
  Flow forwarding mode:
    Inet forwarding mode: packet based
    Inet6 forwarding mode: packet based
    MPLS forwarding mode: packet based
    ISO forwarding mode: packet based
  Flow trace status
    Flow tracing status: off
  Flow session distribution
    Distribution mode: RR-based
  Flow ipsec performance acceleration: off
  Flow packet ordering
    Ordering mode: Hardware
```

Kuva 4.4. *IPv6-pakettien välityksen salliminen pakettikohtaisesti Juniperin reitittimessä R02.*

Kuvasta huomataan, että IPv6-pakettien välitykselle on kolme vaihtoehtoa, joista ensimmäinen estää IPv6-pakettien välityksen reitittimellä, toinen sallii välityksen vuoperusteisesti ja kolmas pakettikohtaisesti. Kuvan alaosassa on esitetty tuloste, josta havaitaan, että IPv6-pakettien välityksen tila (Inet6 forwarding mode) on konfiguroinnin myötä sallittu pakettikohtaisesti, kun se alun perin oli drop-tilassa. Kun IPv6-pakettien välitys on globaalisti sallittu reitittimellä, voidaan liitännöille konfiguroida IPv6-osoitteet. Jotta verkossa olevan Juniperin reitittimen avulla voidaan muodostaa esimerkiksi laboratorioverkossa oleville kytkimille IPv6-hallintaosoitteet tilattomalla autokonfiguraatiolla, täytyy vielä ND-protokolla ottaa erikseen käyttöön reitittimellä. Oletuksena ND-protokollaan liittyvien RA-viestien välittäminen Juniperin reitittimeltä verkon muille laitteille on siis estetty.

Reititin voidaan konfiguroida lähettämään RA-viestejä verkon muille laitteille kuvassa 4.5 esitetyllä konfiguraatiolla.

```
# set protocols router-advertisement interface vlan.777 prefix 2001:2060:bffd:bffd::/64
```

Kuva 4.5. *ND-protokollan käyttöönotto Juniperin reitittimellä.*

Yllä olevan kuvan konfiguraatiossa sallitaan ND-protokollan mainostaa verkon muille laitteille liitännän vlan.777 kautta hallintaverkon prefiksi. Tämän mainostettavan prefiksin avulla verkon muut laitteet, kuten kytkimet voivat generoida itselleen tilattoman autokonfiguraation avulla IPv6-hallintaosoitteen, mikäli kytkimen liitännän konfiguraatiossa osoitteenmuodostustavaksi on valittu tilaton autokonfiguraatio. (Juniper 2014)

Myös Ciscon kytkimissä IPv6-protokolla ei ole automaattisesti tuettu, vaan sen käyttöönotto vaatii erillisiä konfiguraatioita, jotta protokolla saadaan toimimaan laitteissa. Näin ollen esimerkiksi IPv6-hallintaosoitteiden konfigurointi hallintaliitännän alle ei ole mahdollista ennen kuin IPv6-protokolla on globaalisti otettu käyttöön kytkimellä. Ciscon kytkimissä on niin sanottu SDM-ominaisuus (Switch Database Management), jonka avulla kytkimen resursseja voidaan ohjata paremmin tukemaan eri ominaisuuksia. Oletuksena kytkimen resurssien käyttö on tasapainotettu kaikille toiminnoille. SDM-ominaisuuden avulla voidaan lisäksi ottaa käyttöön IPv6-protokolla kytkimessä. Kaikissa laboratorioverkon Ciscon kytkimissä on SDM-komento, jonka lisäparametreilla kytkimessä voidaan sallia sekä IPv4- että IPv6-protokollan samanaikainen käyttö eli niin sanottu dual-stack-toiminto. Kaikkiin laboratorioverkon Ciscon kytkimiin tämä voidaan konfiguroida kuvan 4.6 yläosassa esitetyllä komennolla.

```
(config)#sdm prefer dual-ipv4-and-ipv6 default
(config)#


#show sdm prefer
The current template is "dual-ipv4-and-ipv6 default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.

 number of unicast mac addresses:                  8K
 number of IPv4 IGMP groups + multicast routes:    0.25K
 number of IPv4 unicast routes:                    0
 number of IPv6 multicast groups:                  0.375k
 number of directly-connected IPv6 addresses:      0
 number of indirect IPv6 unicast routes:           0
 number of IPv4 policy based routing aces:         0
 number of IPv4/MAC qos aces:                      0.125k
 number of IPv4/MAC security aces:                 0.375k
 number of IPv6 policy based routing aces:         0
 number of IPv6 qos aces:                          0
 number of IPv6 security aces:                     0.125k
```

Kuva 4.6. *Dual-stack-ominaisuuden konfigurointi Ciscon kytkimeen ja tuloste SDM-ominaisuudesta konfiguroinnin jälkeen.*

Komennon default-parametrilla valitaan, että kytkin käyttää resurssejaan tasapainotetusti sekä IPv4- että IPv6-protokollien toisen ja kolmannen protokollatason toiminnallisuuksiin. Kun kytkimen SDM-ominaisuudessa on sallittu sekä IPv4- että IPv6-protokollan käyttö, vaatii kytkin vielä uudelleenkäynnistyksen, jotta tehdyt muutokset tulevat voimaan. Kuvan 4.6 alaosassa on esitetty tuloste SDM-ominaisuudesta dual-stack-toiminnon käyttöönoton ja laitteen uudelleenkäynnistyksen jälkeen. IPv6-protokollan käyttöönoton jälkeen voidaan kytkimelle konfiguroida IPv6-hallintaosoite. (Cisco 2016b; Cisco 2016c)

HP:n kytkimissä ei tarvitse tehdä vastaavanlaista IPv6-protokollan globaalia käyttöönottoa kuin Ciscon kytkimissä, vaan protokolla on tuettu jo valmiiksi, mikäli laite ja sen ohjelmistoversio ovat IPv6-protokollaa tukevia. Oletuksena IPv6-operaatiot ovat kuitenkin estetty VLAN-tasolla, joten niissä protokolla tulee erikseen sallia. Tietyn VLANin IPv6-operaatiot voidaan sallia VLAN-kohtaisessa konfiguraatiossa joko protokollan erikseen sallivalla komennolla tai määrittämällä VLAN-liitännälle unicast-osoite, jolloin IPv6-operaatiot sallitaan automaattisesti kyseisessä liitännässä. (HP 2016a, s. 9-11; HP 2016b, s. 9-11)

4.3 Globaalien hallintaosoitteiden konfigurointi verkkolaitteisiin

Jokaisella verkkolaitteella tulee hallintayhteyksiä varten olla määritelty laitteen yksilöivä IPv6-hallintaosoite, joka voidaan konfiguroida laitteille joko manuaalisesti tai hyödyntäen IPv6:n tilatonta autokonfiguraatiota. Laboratorioverkossa sijaitsevien reitittimien hallintaosoitteet on muodostettu manuaalisesti konfiguroimalla hyödyntäen laitteiden EUI-64-tunnisteita. Kuvassa 4.7 on esitetty, kuinka Ciscon reitittimelle R01 on muodostettu IPv6-hallintaosoite.

```
        (config)#interface FastEthernet0/1.777
        (config-subif)#ipv6 enable
        (config-subif)#ipv6 address 2001:2060:BFFD:BFFD::/64 eui-64
        (config-subif)#end
        #show ipv6 interface brief fastEthernet 0/1.777
FastEthernet0/1.777        [up/up]
    FE80::213:C3FF:FEC2:AA2B
    2001:2060:BFFD:BFFD:213:C3FF:FEC2:AA2B
```

Kuva 4.7. *IPv6-hallintaosoitteen konfigurointi Ciscon reitittimeen R01.*

Yllä olevassa kuvassa on luotu reitittimen portin FastEthernet0/1 loogiselle aliliitännälle (subinterface) FastEthernet0/1.777 IPv6-hallintaosoite. Työssä käytetään virtuaalista lähiverkkoa 777 kaikkien verkkolaitteiden hallintayhteyksien muodostamiseen. Kuvassa on ensin syötetty komento, joka sallii IPv6-operaatiot yleisesti tässä liitännässä ja generoi automaattisesti link-local-osoitteen tälle liitännälle. Jälkimmäinen komento määrittelee tälle aliliitännälle globaalin unicast-osoitteen, joka muodostetaan komennossa määritellyn prefiksin ja laitteen EUI-64-tunnisteen avulla, joka vastaavasti muodostetaan laitteen

MAC-osoitteesta. Reitittimen hallintaosoite voitaisiin määritellä myös syöttämällä haluttu IPv6-osoite kokonaan ilman, että hyödynnettäisiin EUI-64-menetelmää liitäntätunnisteosan muodostamiseen. Tällöin IPv6-osoitteen konfigurointi liitännälle tapahtuisi vastaavalla tavalla kuin IPv4-osoitteiden konfiguroinnissa. Ainoastaan osoitteistukseen käytettävän IPv6-osoitelohkon verkkomaski syötetään komennossa /<verkkomaski> -muodossa, jossa kauttaviivan jälkeinen luku ilmoittaa osoitelohkon verkkomaskin. (Cisco 2009) Kuvan 4.7 show-komennolla nähdään liitännälle määritetyt IPv6-osoitteet konfiguraatioiden jälkeen, joista ylempi on liitännän link-local- ja alempi globaali unicast-osoite.

Juniper srx-sarjan reitittimelle R02 hallintaosoitteen konfigurointi voidaan tehdä vastaavalla tavalla kuin edellä Ciscon reitittimelle hyödyntäen EUI-64-menetelmää kuvassa 4.8 esitetyllä tavalla.

```
# set interfaces vlan unit 777 family inet6 address 2001:2060:bffd:bffd::/64 eui-64
# exit
> show interfaces terse vlan.777
Interface               Admin Link Proto    Local                 Remote
vlan.777                up    up   inet6    2001:2060:bffd:bffd:fac0:1ff:fe86:7208/64
                                            fe80::fac0:1ff:fe86:7208/64
```

Kuva 4.8. *IPv6-hallintaosoitteen konfigurointi Juniperin reitittimeen R02.*

Kuvassa VLAN-liitännälle konfiguroidaan IPv6-osoite syöttämällä komennon parametriksi hallintaverkon IPv6-prefiksi sekä antamalla komennolle lisäparametriksi tieto, että osoitteen liitäntätunnisteosan muodostamisessa hyödynnetään EUI-64-menetelmää. Kuvan alaosassa suoritetulla show-komennolla esitetään hallintaliitännän globaali unicast- sekä liitännän link-local-osoite, jonka laite muodostaa automaattisesti liitännälle, kun sille määritettään globaali unicast-osoite. (Juniper 2014)

Laboratorioverkon kytkimien hallintaliitäntöjen konfiguroinnissa on testattu, kuinka IPv6-protokollan uutta ominaisuutta tilatonta autokonfiguraatiota voidaan hyödyntää verkkolaitteiden hallintaosoitteiden muodostamiseen. Ciscon kytkimen hallintaliitännässä IPv6-operaatiot voidaan sallia ja sille voidaan määrittää hallintaosoite tilattoman autokonfiguraation avulla kuvassa 4.9 esitetyillä konfiguraatioilla. Alla olevassa kuvassa on esimerkkinä luotu hallintaosoite autokonfiguraation avulla stack-kytkimelle K06.

```
(config)#interface vlan 777
(config-if)#ipv6 enable
(config-if)#ipv6 address autoconfig
(config-if)#end
#show ipv6 interface brief vlan777
Vlan777                 [up/up]
    FE80::216:C7FF:FEB4:1AC2
    2001:2060:BFFD:BFFD:216:C7FF:FEB4:1AC2
```

Kuva 4.9. *IPv6-hallintaosoitteen konfigurointi Ciscon kytkimeen.*

Kuvan konfiguraatiossa ensimmäisellä komennolla sallitaan IPv6-operaatiot VLAN-liitännässä, jonka jälkeen liitännälle konfiguroidaan IPv6-hallintaosoite tilattoman autokonfiguraation avulla. Kuvan tilanteessa toisena syötetty komento luo siis automaattisesti liitännälle hallintaosoitteen sekä tarkastaa tämän osoitteen mahdollisten duplikaattiosoitteiden varalta. Lisäksi kuvan tilanteessa show-komennolla tarkistetaan, onko laite onnistunut automaattisesti generoimaan tälle liitännälle IPv6-osoitteen. Tulosteesta havaitaan, että liitännällä on sekä link-local- että globaali unicast-osoite, jotka laite on onnistunut automaattisesti muodostamaan itselleen. Ciscon kytkimelle hallintaosoite voitaisiin muodostaa myös vastaavalla tavalla kuin kuvassa 4.7 reitittimen R01 konfiguraation kohdalla.

HP:n kytkimiin vastaavat operaatiot ja tilattomaan autokonfiguraatioon liittyvät konfiguraatiot voidaan tehdä kuvassa 4.10 esitetyllä tavalla.

```
          (config)# vlan 777
          (vlan-777)# ipv6 enable
          (vlan-777)# ipv6 address autoconfig
          (vlan-777)# end
          # show ipv6 vlan 777

Internet (IPv6) Service

 IPv6 Routing    : Disabled
 Default Gateway : fe80::213:c3ff:fec2:aa2b%vlan777
 ND DAD          : Enabled
 DAD Attempts    : 3
 Interface Name  : VLAN777
 IPv6 Status     : Enabled
 Layer 3 Status  : Enabled

 IPv6 Address/Prefixlength                   Expiry
 ------------------------------------------- -------------------------
 2001:2060:bffd:bffd:ee9a:74ff:fe12:3ee0/64  Mon Jun 20 12:33:50 2016

 fe80::ee9a:74ff:fe12:3ee0/64                permanent
```

Kuva 4.10. *IPv6-hallintaosoitteen konfigurointi HP:n kytkimeen.*

Kuvan konfiguraatiosta huomataan, että HP:n kytkimien liitäntäkohtaiset autokonfiguraatiokomennot eivät eroa Ciscon vastaavista komennoista. Kuvan tilanteessa VLAN:ssa 777 ensin sallitaan IPv6-operaatiot, jonka jälkeen konfiguroidaan, että VLAN-liitännän IPv6-osoitteen muodostamiseen käytetään tilatonta autokonfiguraatiota. Kuvan viimeisellä komennolla jälleen tarkastetaan, että laite on onnistunut generoimaan VLAN-liitännälle IPv6-hallintaosoitteen. Kuvasta voidaan jälleen huomata, että liitännälle on generoitu automaattisesti sekä globaali unicast- että link-local-osoite. (HP 2016a; HP 2016b) IPv6-hallintaosoitteita konfiguroitaessa havaittiin, ettei yksi laboratorioverkon HP:n kytkimistä K09 tue ollenkaan IPv6-operaatioita, joten tämä kytkin jää pois myöhemmässä vaiheessa suoritettavista tutkimuksista.

Yllä olevissa tilanteissa hallintaosoitteiden konfiguroinnin yhteydessä ei IPv6-protokollan salliminen erillisellä komennolla ole välttämätöntä. Tämä sen takia, koska kuvan tilanteissa globaalien unicast-osoitteiden konfigurointi myös sallii IPv6-protokollan automaattisesti näissä liitännöissä, jolloin erillistä IPv6-operaatiot sallivaa liitäntäkohtaista komentoa ei välttämättä tarvita. Samalla hallintaliitännälle määritellään automaattisesti link-local-osoite, jos sillä ei sitä vielä ole, kun globaali unicast-osoite määritellään joko manuaalisesti konfiguroimalla tai tilattomalla autokonfiguraatiolla. Niin link-local- kuin globaalit unicat-osoitteet voidaan konfiguroida liitännöille myös manuaalisesti ilman, että hyödynnetään automatisoitua osoitteenmuodostusta. Kaikkien kytkimien globaalit hallintaosoitteet voitaisiin konfiguroida myös vastaavalla tavalla kuin Ciscon reitittimen tapauksessa kuvassa 4.7 hyödyntämällä laitteiden EUI-64-tunnisteita. Lisäksi osoitteet voitaisiin konfiguroida myös ilman, että hyödynnetään laitteiden EUI-64-tunnisteita syöttämällä komennon jatkoksi koko IPv6-osoite.

4.4 Verkon IPv6-osoitteistus

Laboratorioverkon verkkolaitteiden hallintaosoitteita varten on varattu IPv6-osoitelohko, josta jaetaan hallintaosoitteet kaikille verkon laitteille. Näiden hallintaosoitteiden tarkoituksena on yksilöidä laboratorioverkon laitteet ja mahdollistaa hallinta- ja valvontayhteyksien muodostaminen niihin.

Laboratorioverkon laitteiden hallintaosoitteita varten varattu IPv6-osoitelohko on 2001:2060:BFFD:BFFD::/64, jolloin IPv6-osoitteiden prefiksin pituus on 64-bittiä. Tämä tarkoittaa sitä, että verkkolaitteiden liitännät yksilöidään 128-bittisen IPv6-osoitteen 64:llä viimeisellä bitillä. Kaikkien laboratorioverkon laitteiden IPv6-osoitteiden liitäntätunnisteosat on luotu käyttäen laitteiden EUI-64-tunnisteita, jotka muodostetaan laitteiden MAC-osoitteiden avulla.

Taulukossa 4.2 on esitetty laboratorioverkossa sijaitsevien verkkolaitteiden globaalit IPv6-hallintaosoitteet, joita käytetään työssä tehtävissä tutkimuksissa. Vasemmanpuoleisessa sarakkeessa on esitetty laitetunnus, jota vastaava hallintaosoite on esitetty oikeanpuoleisessa sarakkeessa.

Taulukko 4.2. *Verkkolaitteiden IPv6-hallintaosoitteet.*

LAITETUNNUS	LAITTEEN IPv6-HALLINTAOSOITE (/64)
R01	2001:2060:BFFD:BFFD:213:C3FF:FEC2:AA2B
R02	2001:2060:BFFD:BFFD:FAC0:1FF:FE86:7208
K01	2001:2060:BFFD:BFFD:21F:6DFF:FE56:28C2
K02	2001:2060:BFFD:BFFD:21F:6DFF:FE56:2042
K03	2001:2060:BFFD:BFFD:DEEB:94FF:FE8F:96C2
K04	2001:2060:BFFD:BFFD:EE9A:74FF:FE12:3EE0
K05	2001:2060:BFFD:BFFD:218:BAFF:FE65:AFC2
K06	2001:2060:BFFD:BFFD:216:C7FF:FEB4:1AC2
K07	2001:2060:BFFD:BFFD:F2B2:E5FF:FE15:447B
K08	2001:2060:BFFD:BFFD:3EA8:2AFF:FE56:8D40
K09	Ei IPv6-tukea

Taulukosta 4.2 nähdään, että kaikille verkossa sijaitseville IPv6-protokollaa tukeville verkkolaitteille niiden hallintaliitäntään on asetettu IPv6-osoite samasta osoitelohkosta. Taulukon reitittimien globaalit hallintaosoitteet on määritetty manuaalisesti konfiguroimalla. Laboratorioverkossa sijaitsevien kytkimien hallintaosoitteiden määrityksessä on hyödynnetty IPv6-protokollan mahdollistamaa autokonfiguraatiota. Reitittimien R01 ja R02 mainostamien verkkoprefiksien avulla kytkimien hallintaliitännöille on saatu määritettyä IPv6-osoitteet konfiguroimalla hallintaliitännän IPv6-osoitteen määritystavaksi autokonfiguraatio. Reitittimet mainostavat tämän alaluvun alussa esitetyn 64-bittisen prefiksin kaikille laboratorioverkon laitteille ND-protokollan avulla. Kun verkkolaitteiden hallintaliitäntöjen konfigurointitavaksi on määritetty tilaton autokonfiguraatio, muodostavat laitteet automaattiset tälle liitännälle 128-bittisen IPv6-osoitteet liittämällä reitittimien mainostaman prefiksin ja liitännän 48-bittisestä MAC-osoitteesta muodostetun 64-bittisen liitäntätunnuksen yhteen. Seurauksena verkkolaitteille saadaan yksilöidyt verkko-osoitteet olettaen, että liitäntöjen MAC-osoitteet ovat uniikkeja, kuten ne tässä työssä ovat.

5. TUTKIMUSTEN TOTEUTTAMINEN

Tässä luvussa käydään läpi työn tutkimusosan tavoitteet. Määritellään tarkemmin, mitä tehtävillä tutkimuksilla halutaan saavuttaa ja minkälaista tietoa niiden perusteella pyritään saamaan. Lisäksi selvitetään, kuinka tutkimukset on suunniteltu toteutettavaksi ja kuinka ne tullaan käytännössä suorittamaan. Lisäksi luvun lopussa esitellään yksityiskohtaisesti tutkimuksessa aikaansaadut tulokset ja tehdään päätelmiä saatujen tulosten perustella protokollan käyttöönotosta verkkolaitteiden hallinnassa ja valvonnassa.

5.1 Tutkimusten tavoitteet

Yleisesti tutkimusten ensisijaisena tavoitteena on selvittää, kuinka työn alkupuolella esitellyt verkkolaitteiden hallinta- ja valvontaprotokollat Telnet, SSH ja SNMP toimivat edellisessä luvussa esitellyssä IPv6-osoitteisessa ympäristössä. Tarkoituksena on löytää vastauksia siihen, voidaanko verkkolaitteiden hallinta- ja valvontayhteydet periaatteellisella tasolla toteuttaa laitteiston ja protokollien puolesta samalla tavalla kuin ne on tällä hetkellä toteutettu vanhemman IPv4-protokollan kanssa. Työn tutkimuksissa keskitytään IPv6-protokollan ja yksittäisten verkkolaitteiden väliseen toimivuuteen. Yksittäisiin verkkolaitteisiin kohdistuvilla tutkimuksilla pyritään löytämään vastauksia erityisesti siihen, voidaanko laitteiden yleisillä IPv6-konfiguraatioilla mahdollistaa vastaavanlainen hallinta- ja valvontayhteyksien toteutus kuin IPv4-protokollalla. Samalla havaiten mahdollisia laitemallikohtaisia rajoituksia liittyen IPv6-protokollalla toteutettuihin yhteyksiin. Lisäksi tutkimuksilla yritetään löytää laitevalmistajien ja -mallien välisiä mahdollisia eroja etäyhteyksien muodostamisessa.

Telnet- ja SSH-protokollien tutkimusten tavoitteena on löytää vastauksia siihen, kuinka etäkirjautuminen toimii verkkolaitteiden IPv6-protokollalla määritettyihin hallintaosoitteisiin, kun yhteydet laitteille muodostetaan etäpalvelimelta. Tällä halutaan selvittää, vaikuttaako osoitteistukseen käytettävä protokolla laitteiden saavutettavuuteen näiden etäkirjautumiseen käytettävien protokollien kohdalla. Tässä yksittäisiin laitteisiin kohdistuvat tutkimukset antavat vastauksia niin laitemallien IPv6-protokollatuesta, mutta myös laitteille ladattujen IPv6-protokollaa tukevien ohjelmistojen toimivuudesta. Lisäksi tutkimuksissa on tarkoitus selvittää, kuinka Telnet- ja SSH-yhteyksien muodostaminen laitteiden välillä toimii. Laitteiden välisillä yhteyksillä tarkoitetaan sitä, miten esimerkiksi reitittimeltä, johon on ensin luotu Telnet- tai SSH-yhteys etäpalvelimelta, voidaan edelleen ottaa yhteys toiseen verkkolaitteeseen, kuten reitittimeen tai kytkimeen. Tällä pyritään löytämään erityisesti eri laitevalmistajien laitteiden välisiin etäyhteyksiin liittyviä mahdollisia ongelmia.

SNMP-protokollan liittyvien tutkimusten tavoitteena on selvittää, kuinka SNMP-yhteydet ja IPv6-protokolla soveltuvat käytettäväksi yhdessä. Lähtökohtana SNMP-tutkimuksille on onnistua lukea laitteilta tilatietoja SNMP-protokollan avulla, kun protokollalla muodostettavien yhteyksien kohteena on verkkolaitteiden IPv6-hallintaosoite. Tämän onnistuessa voidaan varmistua siitä, että protokollat ovat yhteentoimivia. Tarkoituksena on tutkia protokollan eri versioiden toimivuutta yhdessä IPv6-protokollan kanssa.

Normaaleissa käytännön tilanteissa kytkimien etäkirjautumisiin liittyy vahvasti pääsylistat, jotka määrittelevät laitetasolla ne säännöt, joiden mukaan laitteelle sisään tai laitteelta ulos muodostettavat yhteydet joko sallitaan tai estetään. Luoduilla pääsylistoilla voidaan parantaa kytkimien tietoturvallisuutta, kun ainoastaan ennalta määritetyistä ja valtuutetuista lähdeosoitteista tai -verkoista voidaan muodostaa etäyhteyksiä niille ja sitä kautta mahdollisesti päästä näkemään ja muuttamaan laitteiden konfiguraatioita. Etäkirjautumisiin liittyvissä tutkimuksissa tarkastelun kohteena on laitekohtaisten IPv6-protokollaan tukevien pääsylistojen toimivuus ja erityisesti Ciscon ja HP:n kytkimet. Tavoitteena on selvittää, kuinka etäyhteydet laboratorioverkon kytkimille voidaan estää ennalta määritetystä IPv6-kohteesta sekä, kuinka etäyhteydet samaisesta kohteesta vastaavasti voidaan paikallisesti sallia kytkimelle konfiguroitavien pääsylistojen avulla.

5.2 Tutkimusten suunnittelu

Tutkimusosuus voidaan jakaa neljään osaan, joista kolme käsittelee tutkittavien hallinta- ja valvontaprotokollien toimivuuden testaamista IPv6-osoitteisessa ympäristössä. Neljäs tutkimusosa käsittelee sitä, kuinka verkkolaitteiden turvallisuuteen liittyvät pääsylistat toimivat IPv6-protokollan kanssa. Ensimmäisen ja toisen osan tutkimukset kohdistuvat verkonhallintaprotokolliin ja erityisesti etäkirjautumisen mahdollistamiin Telnet- ja SSH-protokolliin. Ensimmäisessä vaiheessa tutkitaan Telnet-protokollan avulla muodostettavien etäyhteyksien toimivuutta kaikkiin laboratorioverkkoon sijoitettuihin verkkolaitteisiin. Toisessa vaiheessa tutkitaan tietoturvallisemmalla SSH-protokollalla muodostettujen etäyhteyksien toimivuutta laitteiden IPv6-protokollalla muodostettuihin hallintaosoitteisiin. Ensimmäisen ja toisen vaiheen tutkimukset käsittävät myös laitteiden välisen kirjautumisen toimivuuden testaamisen. Kolmannen vaiheen tutkimukset liittyvät enemmän verkonvalvontaan käytettävän protokollan eli SNMP:n toimivuuden testaamiseen. Viimeisessä tutkimusosassa on tarkoituksena tehdä kokeiluja, kuinka vastaavanlaiset pääsylistat esimerkiksi verkkolaitteiden etäkirjautumiselle voidaan tehdä IPv6-protokollan tapauksessa kuin ne on nyt tehty IPv4-protokollalla muodostettavien hallintaosoitteiden kanssa.

Kolmeen ensimmäiseen osaan liittyvät tutkimukset suoritetaan perusperiaatteeltaan samalla tavalla. Jokaisen protokollan toimivuutta testataan kaikkien laboratorioverkossa sijaitsevien verkkolaitteiden hallintaosoitteisiin ja näiden testitilanteiden avulla saatujen tulosten pohjalta tehdään päätelmiä IPv6-protokollan toimivuudesta kyseisessä verkkolaitteessa. Kaikkien kolmen protokollan toimivuuden testaus suoritetaan ottamalla kullakin

protokollalla yhteys verkkolaitteen hallintaliitännän IPv6-osoitteeseen. Kahden ensimmäisen osan tutkimuksia laajennetaan vielä laitteiden välisten etäyhteyksien toimivuuden testaamiseen. Tällöin tutkitaan, voidaanko toiselta verkkolaitteelta muodostaa hallintayhteys toiseen verkkolaitteeseen niin sanotusti hyppäämällä laitteelta toiselle Telnet- ja SSH-protokollien avulla. Nämä tutkimukset tullaan suorittamaan siten, että yhteyksien toimivuutta testataan saman laitevalmistajien, mutta myös eri laitevalmistajien laitteiden välillä. Molemmilta laboratorioverkon reitittimiltä testataan etäyhteyksiä sekä Ciscon että HP:n verkkokytkimiin sekä yhteyksiä reitittimien välillä. Lisäksi tutkimuksissa otetaan huomioon myös Ciscon ja HP:n kytkimien välisten yhteyksien toimivuus sekä saman valmistajan eri laitemallien väliset yhteydet.

Kolmannen osan tutkimuksissa tarkoitus on testata, voidaanko virtuaalikoneelle asennetun snmpwalk-työkalun avulla lukea verkkolaitteilta tilatietoja, kun työkalulla muodostetut SNMP-kyselyt lähetetään laitteiden IPv6-hallintaosoitteisiin. Tarkoituksena on testata kaikkien kolmen SNMP-protokollaversion toimivuutta ja testata, voidaanko jokaisella protokollaversiolla lukea tietoja verkkolaitteilta. Mikäli virtuaalikoneelta lähetetyillä kyselyillä onnistutaan tiedustella laitteiden tietoja, voidaan varmistua siitä, että SNMP- ja IPv6-protokolla ovat yhteensopivia ja niiden yhteentoimivuus laajemmin on mahdollista.

Neljännen vaiheen tutkimuksissa ensisijainen tarkastelukohde on siis siinä, kuinka kytkimiin konfiguroitavilla IPv6-pääsylistoilla voidaan sallia ja estää tietyistä kohteista saapuvat etäyhteyksien muodostusyritykset. Tutkimuksissa hyödynnetään Telnet- ja SSH-protokollia vastaavalla tavalla kuin näiden protokollien toimivuuteen liittyvissä tutkimuksissa. Pääsylistojen toimivuutta tutkitaan ainoastaan niihin kytkimiin, joihin on aikaisemmissa tutkimuksissa onnistuttu luomaan etäyhteydet joko Telnet- tai SSH-protokollalla. Pääsylistojen toimivuutta voidaan tutkia siten, että ensin tutkitaan estävän pääsylistan toimivuutta konfiguroimalla kytkimille pääsylistat, jotka estävät virtuaalikoneen IPv6-osoitteesta muodostettavat yhteydet samalla sallien kaikista muista lähteistä saapuvat yhteydet. Pääsylistojen toimivuus voidaan tässä varmistaa yrittämällä ottaa Telnet- tai SSH-yhteys kytkimille, jolloin pääsylistojen tulisi estää tästä lähdeosoitteesta tuleva yhteydet. Sallivan pääsylistan tilanne, jossa halutaan sallia yhteydet kytkimille ainoastaan tietyistä kohteista, voidaan mallintaa asettamalla virtuaalikoneen IPv6-osoite tai -osoiteavaruus sallivien lähdeosoitteiden listaan, jolloin ainoastaan tästä osoitteesta tai verkosta saapuvat yhteydet hyväksytään. Mikäli tutkimus onnistuu, pitäisi etäyhteyksien muodostus kytkimille onnistua toisin kuin tutkimuksen ensimmäisessä vaiheessa.

5.3 Tutkimusten suorittaminen

Tässä alaluvussa käydään läpi, kuinka Telnet-, SSH- ja SNMP-yhteyksiin liittyvät tutkimukset IPv6-osoitteisessä verkkoympäristössä on suoritettu. Ensin käydään läpi, kuinka Telnet-yhteyksien toimivuuden testaaminen virtuaalipalvelimelta verkon laitteille sekä laitteiden välillä on suoritettu. Seuraavaksi käsitellään vastaavat tilanteet SSH-protokol-

lalla suoritettuna. Tämän jälkeen käydään läpi, kuinka SNMP-protokollaan liittyvät tutkimukset on suoritettu laboratorioverkon laitteisiin. Neljännessä vaiheessa esitellään, kuinka verkkolaitteiden turvallisuuteen liittyvät tutkimukset on suoritettu.

5.3.1 Telnet

Telnet-yhteyksien tutkimuksen tarkoituksena on siis testata, kuinka verkkolaitteiden hallintaosoitteisiin voidaan muodostaa etäyhteydet virtuaalipalvelimella sijaitsevalta virtuaalikoneelta. Ennen kuin varsinaiset testaustilanteet suoritetaan, testataan, onko verkossa sijaitseva verkkolaite saavutettavissa virtuaalikoneelle asennetulla ping6-työkalulla. Ping6-työkalun avulla laitteen IPv6-hallintaosoitteeseen voidaan lähettää ICMPv6-paketteja, joihin verkkolaitteelta saatujen vastausten perusteella voidaan päätellä, onko laite saavutettavissa. Mikäli ICMPv6-paketit saavuttavat kohteensa ja testattavalta verkkolaitteelta saadaan vastauksena ICMPv6-paketteja, voidaan sanoa, että verkkolaite on saavutettavissa ja laitteelle on teoriassa mahdollista muodostaa tutkimuksen kohteena olevat hallinta- ja valvontayhteydet kohdistaen yhteydet verkkolaitteen IPV6-osoitteeseen. Kuvassa 5.1 on esitetty havainnollistus siitä, kuinka virtuaalikoneelta voidaan testata esimerkiksi reitittimen R01 saavutettavuutta.

```
user@ubuntu:~$ ping6 2001:2060:BFFD:BFFD:213:C3FF:FEC2:AA2B
PING 2001:2060:BFFD:BFFD:213:C3FF:FEC2:AA2B(2001:2060:bffd:bffd:213:c3ff:fec2:aa2b) 56 data bytes
64 bytes from 2001:2060:bffd:bffd:213:c3ff:fec2:aa2b: icmp_seq=1 ttl=64 time=4.53 ms
64 bytes from 2001:2060:bffd:bffd:213:c3ff:fec2:aa2b: icmp_seq=2 ttl=64 time=0.999 ms
64 bytes from 2001:2060:bffd:bffd:213:c3ff:fec2:aa2b: icmp_seq=3 ttl=64 time=1.05 ms
64 bytes from 2001:2060:bffd:bffd:213:c3ff:fec2:aa2b: icmp_seq=4 ttl=64 time=0.942 ms
```

Kuva 5.1. *Komento, jonka parametrina annetaan verkkolaitteen IPv6-hallintaosoite, voidaan testata virtuaalipalvelimelta laitteen saavutettavuutta.*

Yllä olevassa kuvassa ping6-työkalun avulla lähetetään ICMPv6-paketit kohti reitittimen R01 hallintaliitännän osoitetta 2001:2060:BFFD:BFFD:213:C3FF:FEC2:AA2B. Kuvasta havaitaan, että virtuaalikoneelta lähetettyihin ICMPv6-paketteihin saadaan vastauksia osoitteesta, joka on reitittimen R01 hallintaliitännän osoite. Koska ICMPv6-paketteihin saadaan vastauksia laitteelta, johon ollaan muodostamassa etäyhteyttä, voidaan varmistua siitä, että hallintayhteys Telnet-protokollan avulla tähän osoitteeseen on mahdollista muodostaa, mikäli laite ja sen ohjelmisto tukevat IPv6-protokollaa sekä Telnet-protokollalla muodostettavia hallintayhteyksiä. Vastaavalla tavalla voidaan testata kaikkien laboratorioverkossa sijaitsevien verkkolaitteiden saavutettavuus.

Telnet-tutkimusten suorittaminen tapahtuu siis yksinkertaisella tavalla ottamalla Telnet-yhteys virtuaalipalvelimen tekstipohjaisesta komentorivikäyttöliittymästä verkkolaitteen IPv6-hallintaosoitteeseen. Tämä voidaan suorittaa yksinkertaisella telnet-komennolla, jonka parametrina annetaan testattavan verkkolaitteen IPv6-hallintaosoite. Kuvassa 5.2 on esitetty havainnollistava esimerkki, kuinka virtuaalipalvelimen tekstipohjaiselta ko-

mentorivikäyttöliittymältä voidaan kokeilla ottaa Telnet-yhteys verkkolaitteen hallintaosoitteeseen ja sitä kautta päästä etäkirjautumaan vastaavasti verkkolaitteen tekstipohjaiseen komentorivikäyttöliittymään.

```
user@ubuntu:~$ telnet 2001:2060:BFFD:BFFD:F2B2:E5FF:FE15:447B
Trying 2001:2060:bffd:bffd:f2b2:e5ff:fe15:447b...
Connected to 2001:2060:BFFD:BFFD:F2B2:E5FF:FE15:447B.
Escape character is '^]'.
K07 line 2


User Access Verification

Password:

K07>enable
Password:
K07#
```

Kuva 5.2. *Esimerkki Telnet-yhteyden testaamisesta kytkimeen K07.*

Kuvasta huomataan, että Telnet-yhteys kytkimeen K07 IPv6-hallintaosoitteeseen toimii, koska yhteyden muodostamisen tuloksena onnistutaan kirjautumaan verkkolaitteelle tekstipohjaiseen komentorivikäyttöliittymään. Sisäänkirjautumisen yhteydessä verkkolaite kysyy käyttäjältä tunnistetietoja, jotka vaaditaan, jotta laitteelle voidaan kirjautua sisään. Salasanat on konfiguroitu laitteelle etukäteen estämään valtuuttamattomien henkilöiden etäkirjautuminen verkkolaitteelle. Jokaisen IPv6-protokollaa tukevan laboratorioverkon laitteen Telnet-yhteyksien toimivuuden testaus suoritetaan vastaavalla tavalla muuttaen ainoastaan telnet-komennon IPv6-osoiteparametri vastaamaan testattavan laitteen hallintaosoitetta.

Verkkolaitteiden väliset Telnet-yhteydet testataan vastaavalla tavalla, mutta tällöin yhteys muodostetaan verkkolaitteelta eikä virtuaalipalvelimelta, kuten edellisessä testaustilanteessa. Laitteiden välisiä Telnet-yhteyksiä on testattu saman valmistajien laitteiden välillä, mutta myös eri laitevalmistajien laitteiden välillä.

Kuvassa 5.3 on esitetty esimerkki, kuinka HP:n kytkimeltä K04 on testattu Telnet-yhteyden toimivuutta Ciscon kytkimeen K02.

```
K04# ping6 2001:2060:BFFD:BFFD:21F:6DFF:FE56:2042
2001:2060:bffd:bffd:21f:6dff:fe56:2042 is alive, time = 5 ms
K04# telnet ipv6 2001:2060:BFFD:BFFD:21F:6DFF:FE56:2042

K04  line 2


User Access Verification

Password:

K02>enable
Password:
K02#
```

Kuva 5.3. *HP:n ja Ciscon kytkimien välisen Telnet-yhteyden muodostaminen.*

Kuvan tilanteessa kytkimeltä K04 testataan kytkimen hallintaosoitteen saavutettavuutta vastaavanlaisella ping6-työkalulla kuin virtuaalikoneen tapauksessa. Tämän jälkeen kokeillaan, onnistuuko Telnet-yhteyden muodostaminen näiden laitteiden välillä eli, päästäänkö HP:n kytkimeltä etäkirjautumaan Ciscon kytkimelle. Kuvasta nähdään, että kirjautuminen onnistuu, kun verkkolaitteelle tunnistaudutaan syöttämällä laitteen vaatimat salasanat oikein. Myös muiden laitteiden välisten Telnet-yhteyksien toimivuus voidaan testata vastaavalla tavalla. Ainoastaan laitevalmistajakohtaiset ping- ja telnet-komennot eroavat hieman toisistaan.

5.3.2 SSH

SSH:n avulla voidaan etäkirjautua verkkolaitteille samalla tavalla kuin Telnetin avulla, mutta tietoturvallisin keinoin. Kun Telnetin kohdalla laitteille käyttäjien syöttämät salasanat kulkeutuvat verkkojen yli salaamattomana, SSH:n tapauksessa nämä kulkeutuvat laitteille salattuina. Muutoin SSH-yhteyksien toimivuuden testaus verkkolaitteille suoritetaan perusperiaatteiltaan samalla tavalla kuin Telnet-yhteydet. Kuvassa 5.4 on esitetty, kuinka virtuaalipalvelimelta voidaan muodostaa SSH-yhteys laboratorioverkon laitteelle.

```
user@ubuntu:~$ ssh -l Juniper 2001:2060:bffd:bffd:fac0:1ff:fe86:7208

R02, TeliaSonera Finland Oyj

--- Login using Tacacs+ authentication ---

Password:
--- JUNOS 12.1X46-D40.2 built 2015-09-26 02:25:28 UTC
No alarms currently active

R02>
```

Kuva 5.4. *SSH-yhteys muodostaminen virtuaalipalvelimelta Juniperin reitittimelle R02.*

Kuvan tilanteessa virtuaalipalvelimella on ensin syötetty komento, joka mahdollistaa SSH-yhteyden muodostamiseen esimerkiksi reitittimelle R02. Komennon ensimmäisen parametrin (ssh) jälkeen on syötetty vipu -l, jolla voidaan määrittää käyttäjätunnus, jolla

verkkolaitteelle yritetään kirjautua. Reitittimen R02 tapauksessa käyttäjätunnus on Juniper. Reitittimelle R02 ja kaikille muille laboratorioverkon laitteille on etukäteen konfiguroitu käyttäjätunnus ja tätä vastaava salasana, joita käytetään SSH-yhteyksien muodostamiseen. Komennon viimeisenä parametrina annetaan laitteen IPv6-hallintaosoite, johon yhteyden toimivuutta testataan. Komennon suorittamisen jälkeen huomataan, että yhteys reitittimelle on luotu, jolloin reititin pyytää käyttäjää syöttämään ssh-komennossa syötetyn käyttäjätunnuksen salasanaa. Mikäli salasana vastaa reitittimen konfiguraatiossa määritettyä salasanaa, onnistuu kirjautuminen reitittimelle. Jokaisen laboratorioverkon laitteen SSH-yhteyksien toimivuutta voidaan testata vastaavalla tavalla muutamalla komennossa ainoastaan laitekohtaista käyttäjätunnusta ja hallintaosoitetta.

Verkkolaitteiden välisten SSH-yhteyksien testaaminen suoritetaan vastaavalla tavalla kuin Telnet-yhteyksien testaaminen. Kuvassa 5.5 on esitetty, kuinka reitittimeltä R01, johon ensin otetaan SSH-yhteys virtuaalipalvelimelta, voidaan edelleen ottaa SSH-yhteys toiseen verkkolaitteeseen. Kuvan tilanteessa reitittimeltä otetaan SSH-yhteys HP:n kytkimeen.

```
user@ubuntu:~$ ssh -l Cisco 2001:2060:BFFD:BFFD:213:C3FF:FEC2:AA2B
Password:

R01, TeliaSonera Finland Oyj

R01>ssh -l manager 2001:2060:bffd:bffd:ee9a:74ff:fe12:3ee0
We'd like to keep you up to date about:
  * Software feature updates
  * New product announcements
  * Special events
Please register your products now at:  www.hpe.com/networking/register


manager@2001:2060:bffd:bffd:ee9a:74ff:fe12:3ee0's password:
HP J9623A 2620-24 Switch

K04#
```

Kuva 5.5. *Laitteiden välisten SSH-yhteyksien testaaminen.*

Kuvan tilanteessa on ensin otettu SSH-yhteys virtuaalikoneelta Ciscon reitittimeen R01 vastaavanlaisella komennolla kuin kuvan 5.4 tilanteessa, jossa yhteys muodostettiin Juniperin reitittimeen R02. Kuvan 5.5 tilanteessa ssh-komennon argumenteista edellisen kuvan tilanteeseen verrattuna on vaihdettu ainoastaan käyttäjätunnus vastaamaan Ciscon reitittimelle konfiguroitua käyttäjätunnusta sekä hallintaosoite. Kuvasta huomataan, että SSH-yhteyden muodostus verkkolaitteelle onnistuu sen jälkeen, kun laitteen kysymä salasana syötetään oikein. Nyt Ciscon reitittimeltä voidaan yrittää ottaa edelleen uusi SSH-yhteys toiseen verkkolaitteeseen, mikäli IPv6-protokolla ja laitteet, joiden välille yhteys muodostetaan tukevat protokollia, eikä laitteilla ole estetty SSH-yhteyksien muodostamista pääsylistoilla. Kuvassa Ciscon reitittimeltä on muodostettu uusi SSH-yhteys kytki-

meen K04, jonka käyttäjätunnus ja hallintaosoite on syötetty ssh-komennon argumenteiksi jälkimmäisessä ssh-komennossa. Jälleen HP:n kytkin pyytää käyttäjää tunnistautumaan verkkolaitteelle salasanan avulla. Kun laitteen vaatima salasana syötetään oikein, päästään kirjautumaan verkkolaitteelle. Vastaavalla tavalla voidaan testata myös muiden verkkolaitteiden välisten SSH-yhteyksien toimivuus. Ensin ottamalla SSH-yhteys virtuaalikoneelta jollekin verkon laitteista, josta edelleen ottamalla uusi yhteys toiseen laitteeseen voidaan varmistua laitteiden välisten SSH-yhteyksien toimivuudesta.

5.3.3 SNMP

Verkkolaitteiden hallinta- ja valvontaprotokollaan SNMP:hen liittyvät tutkimukset suoritetaan yksinkertaisella virtuaalikoneelle asennetulla snmpwalk-työkalulla. Työkalun avulla voidaan mallintaa SNMP-protokollan Get-request-kyselyjä. Toisin sanoen työkalun avulla voidaan lähettää verkkolaitteille kyselyitä, joilla tiedustellaan erilaisia verkkolaitteiden hallintaan liittyvien hallintaobjektien arvoja. Kyselyt kohdistetaan jälleen verkkolaitteiden IPv6-hallintaosoitteisiin ja mahdollisten vastausten perusteella tehdään päätelmiä protokollien yhteentoimivuudesta. Alla olevassa kuvassa 5.6 on esitetty, kuinka virtuaalikoneelta voidaan lähettää snmpwalk-komennolla tiedustelu laboratorioverkon laitteille SNMP-protokollan ensimmäisellä versiolla.

```
user@ubuntu:~$ snmpwalk -v 1 -c nocLabra udp6:[2001:2060:BFFD:BFFD:DEEB:94FF:FE8F:96C2] sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software, C2960S Software (C2960S-UNIVERSALK9-M), Version
12.2(55)SE10, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 11-Feb-15 11:59 by prod_rel_team
```

Kuva 5.6. *SNMP-kyselyiden lähettäminen snmpwalk-työkalulla verkkolaitteelle K03 snmpwalk-protokollan versiolla yksi.*

Kuvan tilanteessa snmpwalk-komennon lisäargumenteiksi on syötetty ensin SNMP-versio, joka kuvan tilanteessa on protokollan ensimmäinen versio ja tähän liittyvä vipu -v. Tämän jälkeen komennossa on vipu -c, jolla määritetään SNMP-yhteisön tunniste (community), joka on määritelty kaikille laboratorioverkon laitteille etukäteen laitteiden konfiguraatioissa. SNMP-yhteisöllä voidaan rajata oikeudet hallinta-agenttien ja -asemien välille. Ainoastaan oikeilla SNMP-kyselyviestien mukana siirrettävillä yhteisön merkkijonoilla voidaan laitteelta lukea tai laitteelle kirjoittaa tietoja. (Case et al. 1990) Komennossa on lisäksi syötetty esimerkkilaitteen IPv6-hallintaosoite, jolle komennon kysely halutaan kohdistaa. Komennon viimeisenä argumenttina on syötetty pyydettävän objektin tunnus OID (Object Identifier), joka yksilöi MIB-tietokantaan tallennettavat objektit. Kuvan tilanteessa laitteen MIB-tietokannasta luetaan sysDescr0-nimisen objektin arvoa, joka palauttaa merkkijonotyyppisen tiedon muun muassa laitemallista ja laitteen ohjelmistoversiosta. Verkkolaitteelta vastaanotetun OID-arvon tulosteen perusteella voidaan

varmistua siitä, että käyttäen SNMP-protokollan ensimmäistä versiota on onnistuttu hakea tietoja verkkolaitteen MIB-tietokannasta, kun SNMP-kysely on kohdistettu laitteen IPv6-hallintaosoitteeseen.

Vastaavan tiedon lukemista laitteelta voidaan yrittää myös käyttämällä SNMP-protokollan toista versiota, josta käytetään snmpwalk-komennon yhteydessä merkintää 2c. Kuvassa 5.7 on esitetty vastaava komento kuin kuvassa 5.6, mutta SNMP-protokollan toisella versiolla toteutettuna.

```
user@ubuntu:~$ snmpwalk -v 2c -c nocLabra udp6:[2001:2060:BFFD:BFFD:DEEB:94FF:FE8F:96C2] sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software, C2960S Software (C2960S-UNIVERSALK9-M), Version
12.2(55)SE10, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 11-Feb-15 11:59 by prod_rel_team
```

Kuva 5.7. *SNMP-kyselyn lähettäminen snmpwalk-työkalulla verkkolaitteelle K03 SNMP-protokollan versiolla kaksi.*

Kuvasta huomataan, että SNMP-protokollan toisella versiolla saadaan tulostettua vastaava OID-arvo kuin kuvan 5.6 tilanteessa. SNMP-kyselyyn liittyvät komennot kahdessa edellisessä kuvassa eivät eroa toisistaan muuten kuin snmpwalk-työkalun käyttävän protokollaversion määrityksen osalta.

Protokollan kolmannen version snmpwalk-komento eroaa kahdesta edellisestä huomattavasti jo sen takia, ettei tässä protokollaversiossa hyödynnetä enää SNMP-yhteisötunnistetta, vaan tunnistautuminen tehdään muilla tavoin. Lisäksi SNMPv3 tarjoaa turvallisuuteen liittyviä ominaisuuksia, kuten luvussa 2.4.2 käsiteltiin. Kun nämä turvallisuuteen liittyvät ominaisuudet ovat käytössä laitteella, vaaditaan komennon argumenteiksi myös nämä ominaisuudet määrittelevät osat. Kuvassa 5.8 on esitetty, kuinka virtuaalikoneelta voidaan lähettää SNMPv3-kyselyitä laboratorioverkon verkkolaitteelle.

```
user@ubuntu:~$ snmpwalk -v 3 -l AuthPriv -u testi -a md5 -A snmptesti -x aes -X salausteksti udp6:[2001:2060
:BFFD:BFFD:DEEB:94FF:FE8F:96C2] sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software, C2960S Software (C2960S-UNIVERSALK9-M), Version 12.2(55
)SE10, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 11-Feb-15 11:59 by prod_rel_team
```

Kuva 5.8. *SNMP-kyselyn lähettäminen snmpwalk-työkalulla verkkolaitteelle K03 SNMP-protokollan versiolla kolme.*

Kuvan komento eroaa selvästi kahdesta aiemmasta johtuen kolmannen protokollaversion eroavaisuuksista verrattuna kahteen aikaisempaan versioon. Komennon alkuosa on samanlainen kuin kahdessa ensimmäisessä. Nyt käytettävä protokollaversio ilmaistaan numerolla 3 vivun -v jälkeen. Numeron kolme jälkeinen vipu -l määrittää turvallisuustason, joka on konfiguroitu hallittavalle laitteelle, johon kysely lähetetään. Komennossa laitteiden turvallisuustasoksi on kolme vaihtoehtoa: NoAuthNoPriv, AuthNoPriv ja AuthPriv.

Näistä ensimmäinen taso tarkoittaa kommunikointia hallinta-aseman ja agenttilaitteen välillä, joka ei vaadi autentikaatiota eikä liikenteen salausta. Toinen taso vastaa samanlaista tasoa kuin kahdessa aikaisemmassa protokollaversiossa. Tällöin ainoastaan autentikaatio on käytössä, mutta liikennettä ei salata. Kolmas ja kaikkein turvallisin taso käsittää sekä autentikaation ja salauksen. Kuvan tilanteessa laitteella on käytössä kolmas turvallisuustaso, jolloin SNMPv3-kyselyn lähettämän osapuolen tulee autentikoitua agentille. Tällöin autentikoitumista varten komennossa tulee määrittää käyttäjätunnus, joka on määritelty komennossa argumentin -u jälkeen. Lisäksi autentikointiprotokolla, jota autentikoinnissa käytetään, tulee määrittää osana komentoa. Kuvan tilanteessa käytetään md5-protokollaa, joka annetaan vivun -a jälkeen. Autentikoinnissa tarvitaan käyttäjätunnusta vastaava salasana, joka on konfiguroitu verkkolaitteelle yhdessä käyttäjätunnuksen kanssa. Komennossa tämä ilmaistaan lisäargumentilla -A ja tätä seuraavalla merkkijonolla, joka määrittää autentikoinnissa tarvittavan salasanan. Komennon lopussa on vielä määritetty salausprotokolla, jota käytetään SNMP-viestien salaukseen. Argumentin -x jälkeinen protokolla määrittää käytettävän salausprotokollan. Kuvan tilanteessa käytetään AES-salausta (Advanced Encryption Standard) ja tätä vastaava yksityinen salausavain määritellään merkkijonona argumentin -X jälkeen. Mikäli verkkolaitteella olisi käytössä jompikumpi kahdesta muusta turvallisuustasosta, ei kaikkia komennon lisäargumentteja tarvita. AuthNoPriv-turvallisuustaso käsittää siis ainoastaan autentikoinnin, jolloin snmpwalk-komennon argumenteista voidaan jättää pois salaukseen liittyvät osat. NoAuthNoPriv ei vastaavasti käsitä kumpaakaan turvallisuusominaisuutta, joten komennosta voidaan jättää pois sekä salaukseen että autentikointiin liittyvät osat. Tällöin komennossa ainoa tarvittava tunnistautumiseen liittyvä tieto on vivun -u jälkeen määriteltävä käyttäjä, joka laitteelle on konfiguroitu.

5.3.4 Pääsylistat

Jokaiselle laboratorioverkon kytkimelle, johon on aiemmissa tutkimuksissa onnistuttu etäkirjautumaan joko Telnet- tai SSH-protokollalla käyttäen kohdeosoitteena verkkolaitteen IPv6-hallintaosoitetta, konfiguroidaan ensin pääsylista, joka estää kaikki verkosta 2001:2060:BFFD:BFFD::/64 muodostetut etäkirjautumisyritykset. Edellä mainitusta IPv6-verkosta on jaettu verkko-osoite myös laboratorioverkon virtuaalikoneelle. Samalla pääsylistaan lisätään sääntö, jossa sallitaan kaikista muista IPv6-lähdeosoitteista saapuvat yhteydet, koska ainoastaan yksi kieltävä sääntö pääsylistassa esimerkiksi Ciscon kohdalla hylkäisi muuten kaikki laitteelle saapuvat yhteydet.

Kuvassa 5.9 on esitetty erääseen laboratorioverkon kytkimeen kohdistettu pääsylistan toimivuuden testaus, kun sille on konfiguroitu pääsylista, joka estää virtuaalikoneelle asetetun IPv6-osoitteen osoiteavaruudesta saapuvat yhteydet.

```
user@ubuntu:~$ ping6 2001:2060:BFFD:BFFD:21F:6DFF:FE56:28C2
PING 2001:2060:BFFD:BFFD:21F:6DFF:FE56:28C2(2001:2060:bffd:bffd:21f:6dff:fe56:28c2) 56 data bytes
64 bytes from 2001:2060:bffd:bffd:21f:6dff:fe56:28c2: icmp_seq=1 ttl=64 time=1.21 ms
64 bytes from 2001:2060:bffd:bffd:21f:6dff:fe56:28c2: icmp_seq=2 ttl=64 time=1.10 ms
64 bytes from 2001:2060:bffd:bffd:21f:6dff:fe56:28c2: icmp_seq=3 ttl=64 time=1.61 ms
^C
--- 2001:2060:BFFD:BFFD:21F:6DFF:FE56:28C2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.109/1.313/1.617/0.219 ms
user@ubuntu:~$
user@ubuntu:~$
user@ubuntu:~$ ssh -l Cisco 2001:2060:BFFD:BFFD:21F:6DFF:FE56:28C2
ssh: connect to host 2001:2060:bffd:bffd:21f:6dff:fe56:28c2 port 22: Connection refused
```

Kuva 5.9. *IPv6-pääsylistan testaus, kun virtuaalikoneen IPv6-osoiteesta muodostetut yhteydet on estetty verkkolaiteeseen konfiguroidussa pääsylistassa.*

Kuvasta huomataan, kun virtuaalikoneelta yritetään muodostaa SSH-yhteys kytkimelle K01, estää se etäkirjautumisen. Koska etäyhteyden muodostus kytkimelle ei kuvan tilanteessa onnistu, voidaan varmistua siitä, että pääsylistan lisääminen kytkimen konfiguraatioon aiheuttaa virtuaalikoneelta muodostettavien SSH-yhteyksien estämisen kyseiselle kytkimelle. IPv6-protokollalle määritetyssä pääsylistassa ainoana yhteydet estävänä sääntönä on virtuaalikoneen IPv6-osoiteavaruudesta saapuvat yhteydet, joten voidaan olla varmoja siitä, että pääsylista toimii vastaavalla tavalla myös IPv6-protokollan kohdalla kuin IPv4-protokollalla toteutettuna. Kytkimille voidaan luoda myös päinvastaisia pääsylistoja, jotka sallivat tietyistä lähdeverkoista tai tietystä yksittäisestä IP-osoitteesta muodostettavat etäyhteydet. Pääsylistojen testauksen toisessa vaiheessa kytkimille luodaan pääsylista, jossa sallitaan ainoastaan virtuaalikoneen IPv6-osoitteesta saapuvat yhteydet. Sama lopputulos saavutettaisiin myös, jos verkko johon virtuaalikoneen IPv6-osoite kuuluu, sallittaisiin pääsylistassa. Nyt jokaiselle kytkimelle voidaan yrittää muodostaa etäyhteys virtuaalikoneelta ja yhteyden muodostuksen pitäisi onnistua, mikäli listat toimivat IPv6-protokollalla toteutettuna oikein. Kytkimille konfiguroiduista etäyhteydet sallivista ja estävistä pääsylistoista esitetään esimerkein työn lopussa liitteessä A. Liitteessä esitetään esimerkit Ciscon ja HP:n pääsylistojen konfiguraatioista, joita tutkimuksissa käytetään kaikissa saman laitevalmistajan laitteissa.

5.4 Tulokset

Kolmessa seuraavassa alaluvussa käsitellään tarkemmin aikaisemmissa luvuissa tehtyjen tutkimusten tuloksia. Ensin esitellään Telnet- ja SSH-protokollien toimivuuteen liittyvien tutkimusten tulokset, jonka jälkeen käydään läpi SNMP-tutkimuksissa aikaansaatuja tuloksia. Lopuksi käydään läpi vielä pääsylistoihin liittyvissä tutkimuksissa havaittuja asioita.

5.4.1 Telnet ja SSH

Ensimmäisessä luvussa esitettyjen tutkimuskysymysten mukaan telnet- ja SSH-tutkimusten tavoitteena oli selvittää, voidaanko verkkolaitteille muodostaa etäyhteydet vastaavalla tavalla näiden protokollien avulla, kun hallintaosoitteistuksessa käytetään IPv4-protokollan sijaan IPv6-protokollaa. Selvittää, liittyykö näiden protokollien käyttöön joitakin rajoitteita, jotka voisivat vaikuttaa hallintayhteyksien muodostamiseen IPv6-verkkoympäristössä. Lisäksi tavoitteena oli selvittää eri laitevalmistajien ja -mallien välisiä eroja hallintayhteyksien muodostamisessa.

Taulukossa 5.1 on esitetty jokaiseen laboratorioverkon laitteeseen kohdistettujen Telnet- ja SSH-protokolliin liittyvien tutkimusten tulokset. Taulukossa vasemmanpuoleisessa sarakkeessa on esitetty laboratorioverkon laitteiden tunnukset, keskimmäisessä sarakkeessa tieto siitä, onko Telnet-protokollalla onnistuttu muodostamaan hallintayhteys laitteeseen ja oikeanpuoleisessa sarakkeessa tieto siitä, onko vastaavasti SSH-protokollalla onnistuttu muodostamaan hallintayhteys kyseiseen verkkolaitteeseen, kun kohdeosoitteina on käytetty laitteiden IPv6-hallintaosoitteita.

Taulukko 5.1. *Hallinta- ja valvontaprotokollien avulla muodostettujen yhteyksien toimivuus laboratorioverkon laitteisiin.*

Laitetunnus	***Onnistunut Telnet-yhteyden muodostus verkkolaitteelle***	***Onnistunut SSH-yhteyden muodostus verkkolaitteelle***
R01	Kyllä	Kyllä
R02	Kyllä	Kyllä
K01	Kyllä	Kyllä
K02	Kyllä	Kyllä
K03	Kyllä	Kyllä
K04	Kyllä	Kyllä
K05	Kyllä	Kyllä
K06	Kyllä	Kyllä
K07	Kyllä	Kyllä
K08	Kyllä	Kyllä

K09	Ei (laitteella ei IPv6-tukea)	Ei (laitteella ei IPv6-tukea)

Yllä esitetystä taulukosta huomataan, että jokaiseen laboratorioverkon laitteeseen lukuun ottamatta kytkintä K09 on onnistuttu muodostamaan sekä Telnet- että SSH-yhteys laboratorioverkossa sijaitsevalta virtuaalikoneelta. Lisäksi taulukosta selviää myös syy siihen, miksi kytkimelle K09 ei onnistuttu muodostamaan IPv6-protokollalla toteutettuja hallintayhteyksiä. Kaikki muut laboratorioverkon laitteet lukuun ottamatta kytkintä K09 ovat IPv6-protokollaa tukevia, minkä takia kytkimelle K09 ei voida muodostaa IPv6-hallintaosoitetta eikä hallintayhteyksiä voida siten toteuttaa käyttäen IPv6-protokollaa. Kytkin K09 on vanhempaa HP:n 2610-sarjaa oleva kytkin, jonka tilalle korvaavaksi laitteeksi on kehitetty uudempi 2620-sarjan kytkin, joka tutkimusten mukaan vastaavasti tukee IPv6-protokollaa. Laboratorioverkossa sijaitseva kytkin K04 on tällainen 2620-sarjan kytkin, jolle onnistuttiin kirjautumaan sekä Telnet- että SSH-protokollien avulla.

Ainoa laite, johon ei onnistuttu muodostamaan hallintayhteyksiä kummallakaan etäyhteysprotokollalla ei siis tue IPv6-protokollaa, joten tulosten perusteella voidaan sanoa, että kaikki IPv6-protokollaa tukevat laitteet tukevat hyvin sekä Telnet- että SSH-protokollia yhdessä IPv6-protokollan kanssa. IPv6-protokollatukeen verraten tutkimuksissa saadut tulokset ovat varsin odotettuja. Tulokset ovat varsin odotettuja senkin takia, että laboratorioverkon laitekanta koostuu pääosin melko uusista laitteista, joten on odotettua, että IPv6-protokolla on tuettu suurimmassa osassa laitteita ja siten etäyhteysprotokollat toimivat verkkolaitteilla IPv4-protokollan tavoin myös IPv6-protokollalla. Etäyhteysprotokollien käytössä ei havaittu minkäänlaisia rajoitteita, jotka voisivat vaikuttaa laitteille muodostettaviin IPv6-protokollalla toteutettuihin hallintayhteyksiin. Tehdyt tutkimukset osoittivat, että etäyhteyksien muodostaminen laitteille toimii samalla tavalla riippumatta siitä, onko verkkolaitteiden hallintaosoitteistuksessa käytetty IPv4- vai IPv6-protokollaa. Lisäksi eri laitevalmistajien ja -mallien välillä ei vaikuttaisi olevan juurikaan vaikutusta, koska jokaiselle eri laitevalmistajan kaikille IPv6-protokollaa tukeville verkkolaitteille onnistuttiin muodostamaan hallintayhteydet molempia protokollia käyttäen. Ainoastaan laitekohtaiset IPv6-konfiguraatiot hallintayhteyksien muodostamiseen, joita käsiteltiin tarkemmin luvussa neljä eroavat hieman IPv4-toteutuksista.

5.4.2 SNMP

SNMP-tutkimusten tavoitteena oli selvittää, onnistutaanko SNMP-protokollalla lukea verkkolaitteilta hallintatietoja, kun laitteiden hallintaosoitteistuksessa käytetään IPv6-prorokollaa. Tavoitteina oli lisäksi selvittää mahdollisia rajoittavia tekijöitä sekä löytää mahdollisia eroavaisuuksia eri laitevalmistajien ja -mallien välillä protokollan käytössä.

SNMP-protokollan tutkimukset suoritettiin kolmessa osassa testaten erikseen jokaisen protokollaversion toimivuutta kaikkiin laboratorioverkon laitteisiin. Taulukossa 5.2 on esitetty tulokset jokaisen verkkolaitteen ja eri SNMP-versioiden välillä. Taulukossa ensimmäisessä sarakkeessa on esitetty laboratorioverkon laitteiden tunnukset ja kolmessa seuraavassa sarakkeessa esitetty tieto siitä, onko tietyssä sarakkeessa kuvatulla SNMP-protokollan versiolla onnistuttu lukemaan kyseiseltä verkkolaitteelta hallintatietoja.

Taulukko 5.2 *Eri SNMP-protokollan versioilla muodostettujen yhteyksien toimivuus laboratorioverkon laitteisiin.*

Laitetunnus	***Tietojen lukeminen verkkolaitteelta onnistunut SNMPv1-protokollalla***	***Tietojen lukeminen verkkolaitteelta onnistunut SNMPv2-protokollalla***	***Tietojen lukeminen verkkolaitteelta onnistunut SNMPv3-protokollalla***
R01	Kyllä	Kyllä	Kyllä
R02	Kyllä	Kyllä	Kyllä
K01	Kyllä	Kyllä	Kyllä
K02	Kyllä	Kyllä	Kyllä
K03	Kyllä	Kyllä	Kyllä
K04	Kyllä	Kyllä	Kyllä
K05	Kyllä	Kyllä	Kyllä
K06	Kyllä	Kyllä	Kyllä
K07	Kyllä	Kyllä	Kyllä
K08	Kyllä	Kyllä	Kyllä
K09	Ei (laitteella ei IPv6-tukea)	Ei (laitteella ei IPv6-tukea)	Ei (laitteella ei IPv6-tukea)

Taulukosta nähdään, että tulokset ovat vastaavat kuin edellä Telnet- ja SSH-protokolliin liittyvissä tutkimuksissa. Jokaiselta laboratorioverkon laitteelta lukuun ottamatta kytkintä K09, joka ei tue IPv6-protokollaa on saatu onnistuneesti luettua hallintatietoja jokaisella testattavalla SNMP-protokollan versiolla.

Kuten edellisessä alaluvussa, myös SNMP-tutkimuksissa saadut tulokset ovat varsin odotettuja, koska kaikissa IPv6-protokollaa tukevissa verkkolaitteissa ei havaittu minkäänlaisia ongelmia SNMP- ja IPv6-protokollien yhteentoimivuudessa. Yleisesti SNMP-protokollaan liittyvistä tutkimuksista voidaan sanoa, ettei eri SNMP-versioilla näiden verkkolaitteiden kohdalla ole ongelmaa luettaessa hallintatietoja verkkolaitteilta käyttäen verkkolaitteiden hallintaosoitteistuksessa IPv6-protokollaa. Tehtyjen tutkimusten yhteydessä ei myöskään havaittu minkäänlaisia rajoittavia tekijöitä, jotka voisivat vaikuttaa SNMP-protokollan toimintaan yhdessä IPv6-protokollan kanssa, vaan vaikuttaisi, että protokollalla on edellytykset toimia samalla tavalla riippumatta siitä, onko verkkolaitteiden hallintaosoitteistuksessa käytetty kumpaa IP-protokollaa. Myöskään eri valmistajien verkkolaitteiden eikä saman laitevalmistajan eri mallisten verkkolaitteiden välillä havaittu eroavaisuuksia protokollan toiminnassa.

5.4.3 Pääsylistat

Kytkimien IPv6-pääsylistoihin kohdistuvissa tutkimuksissa ei havaittu minkäänlaisia ongelmia listojen toimivuudessa, vaan pääsylistat toimivat tarkastelun kohteina olevissa kytkimissä odotetulla tavalla. Jokaiselle laboratorioverkossa sijaitsevalle kytkimelle, johon aikaisemmissa tutkimuksissa onnistuttiin etäkirjautumaan joko Telnet- tai SSH-protokollan avulla, onnistuttiin konfiguroimaan IPv6-protokollalla toteutetut pääsylistat. Pääsylistojen testauksen ensimmäisessä vaiheessa listaan luotiin siis säännöt, jotka estivät kaikki yhteydet siitä IPv6-verkosta, josta on jaettu osoite myös laboratorion virtuaalikoneelle, mutta salli kaikista muista lähteistä saapuvat yhteydet. Jokaisen kytkimen kohdalla tämä lista esti etäkirjautumisen, kun kytkimelle yritettiin muodostaa yhteys virtuaalikoneelta joko Telnet- tai SSH-protokollalla. Tehdyillä tutkimuksilla voidaan varmistua siitä, että kaikkiin laboratorioverkossa sijaitseviin IPv6-protokollaa tukeviin kytkimiin voidaan luoda onnistuneesti listoja, joilla saadaan estettyä tietyistä verkoista tai jopa yksittäisestä osoitteesta muodostettavat Telnet- tai SSH-yhteydet.

Pääsylistatutkimusten toisessa vaiheessa edellisessä vaiheessa luodun listan säännöistä muodostettiin päinvastaiset, joka salli ainoastaan virtuaalikoneen osoiteavaruudesta saapuvat yhteydet estäen kaikista muista lähteistä saapuvat etäkirjautumiset. Myös tässä tilanteessa konfiguroitu pääsylista toimi odotetulla tavalla. Nyt virtuaalikoneen lähdeosoitteesta onnistuttiin kirjautumaan jokaiselle IPv6-protokollaa tukevalle kytkimelle eli kaikille muille paitsi kytkimelle K09. Tämän listan toiminnan varmistaminen on kytkimien hallinnan kannalta oleellista, koska usein kytkimien konfiguraatioihin halutaan määrittää juuri ne tietyt lähdeverkot, joista laitteille on mahdollista etäyhteyksiä. Tällä voidaan helposti estää kaikki sellaiset etäkirjautumisyritykset, jotka eivät saavu laitteille esimerkiksi

erilliseltä etähallintapalvelimelta. Pääsylistatutkimusten toisen vaiheen tarkoituksena oli mallintaa edellä mainittua tilannetta, jossa kytkimille voidaan määrittää ainoastaan yksi lähdeverkko tai -osoite, josta yhteydet sallitaan.

Koska jokaiselle laboratorioverkon IPv6-protokolla tukevalle kytkimelle onnistuttiin konfiguroimaan tietystä kohteesta saapuvia etäyhteyksiä varten sekä yhteydet estävät että sallivat pääsylistat, ovat sekä Ciscon että HP:n kytkimet pääsylistojen osalta myös protokollaa tukevia, joten protokollan käyttöönotto hallintaosoitteistuksessa on tältä osin mahdollista ja turvallista. Näin ollen kytkimien konfiguraatioilla voidaan rajoittaa Telnet- ja SSH-protokollilla luotavia etäyhteyksiä samalla tavalla kuin IPv4-protokollalla toteutettuna.

6. YHTEENVETO

Johdantoluvussa työlle määritettiin päätutkimusongelma, jonka tavoitteena oli selvittää, kuinka verkkolaitteiden hallinta- ja valvontayhteydet voidaan toteuttaa IPv6-osoitteisessa verkkoympäristössä. Johdantoluvussa määriteltiin lisäksi useampi tutkimuskysymys, joiden tarkoituksena oli auttaa löytämään vastauksia määriteltyyn päätutkimusongelmaan. Työn tavoitteena olikin vastata päätutkimusongelman pohjalta määritettyihin tutkimuskysymyksiin ja sitä kautta pystyä vastaamaan päätutkimusongelmaan.

Työssä tehtäviä tutkimuksia varten rakennettiin erityinen laboratorioympäristö, joka muodostettiin useista erityyppisistä verkkolaitteista. Tutkimusympäristöön valikoitujen verkkolaitteiden tarkoituksena oli mallintaa mahdollisimman hyvin todellisia lähiverkkoympäristöjä laitteiston osalta, jotta tutkimuksissa saatuja tuloksia voitaisiin käyttää suoraan mahdollisiin jatkotutkimuksiin ja niihin laitteisiin, joita käytetään nykyään laajalti myös organisaatioiden todellisissa verkkoympäristöissä.

Neljännessä luvussa etsittiin vastauksia kahteen ensimmäiseen tutkimuskysymykseen, joissa määriteltiin, kuinka tutkittavissa verkkolaitteissa voidaan ottaa käyttöön IPv6-protokolla ja miten verkkolaitteille voidaan luoda IPv6-protokollalla toteutetut hallintaosoitteet, joita hyödynnetään muodostettaessa yhteyksiä laboratorioverkon laitteille työssä tutkittavilla hallinta- ja valvontaprotokollilla. Neljännen luvun tavoitteena oli selvittää ne verkkolaitteet, joissa ylipäätään voidaan ottaa IPv6-protokolla käyttöön ja tämän jälkeen luoda näille verkkolaitteille IPv6-hallintaosoitteet. Luvussa onnistuttiin hyvin vastaamaan johdantoluvussa määriteltyihin tutkimuskysymyksiin. Tehdyillä käytännön kokeiluilla saatiin selville ne laboratorioverkon laitteet, jotka tukevat IPv6-protokollaa ja lopulta näille onnistuttiin konfiguroimaan IPv6-hallintaosoitteet viidennessä luvussa tehtäviä tutkimuksia varten. Lopputuloksena saatiin hyvä ymmärrys siitä, kuinka Ciscon kytkimissä ja reitittimissä, HP:n kytkimissä sekä Juniperin reitittimissä voidaan ottaa IPv6-protokolla käyttöön ja minkälaisia konfiguraatioita laitteet vaativat, jotta hallintaosoitteistus voidaan toteuttaa IPv6-protokollalla. Samalla testaten IPv6-protokollan uusia ominaisuuksia, kuten tilatonta autokonfiguraatiota, jolla onnistuttiin automaattisesti luomaan osalle laitteista IPv6-hallintaosoitteet. Luvussa havaittiin, että ainoastaan yksi laboratorioverkon laitteista ei tue ollenkaan uudempaa IP-protokollaa. Kyseinen kytkin oli HP:n valmistama 2610-sarjan kytkin.

Viidennessä luvussa suoritetuilla tutkimuksilla selvitettiin kolmen hallinta- ja valvontaprotokollan Telnetin, SSH:n sekä SNMP:n toimivuutta IPv6-osoitteisessa verkkoympäristössä. Luvussa tehdyillä tutkimuksilla pyrittiin vastaamaan kolmeen viimeiseen tutkimuskysymykseen, joissa tavoitteina oli löytää vastauksia siihen, toimivatko kaikki tutkittavat verkkolaitteiden hallinta- ja valvontaprotokollat IPv6-osoitteisessa verkkoympäristössä, kuinka kytkimille luotavat etäyhteyksiä sallivat ja estävät pääsylistat toimivat IPv6-

protokollalla toteutettuna sekä löytää mahdollisia eroavaisuuksia hallinta- ja valvontayhteyksien toteuttamisessa tutkittavien eri valmistajien laitteiden ja eri laitemallien välillä. Tutkimuksissa saatujen tulosten perusteella IPv6-protokollaa tukevan verkkolaitteen näkökulmasta ei näytä olevan merkitystä, onko hallintaosoitteistus toteutettu IPv4- vai IPv6-protokollalla. Kaikissa testitilanteissa jokainen laboratorioverkon IPv6-protokollaa tukeva laite toimi samalla tavalla yhdessä tutkittavan hallinta- tai valvontaprotokollan kanssa kuin tällä hetkellä IPv4-protokollalla toteutettuna, joten laitetasolla protokollien yhteentoimivuus ei näyttäisi riippuvan verkkolaitteissa käytettävästä IP-protokollasta. Tutkimuksissa ei havaittu minkäänlaisia rajoittavia tekijöitä hallinta- ja valvontayhteyksien toteuttamisessa IPv6-protokollalla verrattuna IPv4-protokollan toteutukseen. Myöskään IPv6-protokollalla toteutettujen pääsylistojen kanssa ei havaittu minkäänlaisia ongelmia, vaan kytkimille konfiguroitujen pääsylistojen avulla onnistuttiin sekä estämään että sallimaan tietystä IPv6-osoitteesta saapuvat Telnet- ja SSH-yhteydet samalla tavalla kuin IPv4-protokollalla luoduilla kytkimien pääsylistoilla.

Luvussa viisi tehdyillä tutkimuksilla onnistuttiin vastaamaan kaikkiin lukua koskeviin tutkimuskysymyksiin. Tutkimuksilla saatiin hyvä kuva varsinkin Ciscon ja HP:n kytkimien IPv6-ominaisuuksien toiminnasta yhdessä eri hallinta- ja valvontaprotokollien kanssa. Tulosten perusteella voidaan sanoa, että näiden valmistajien uusimmat kytkinmallit ja ohjelmistoversiot näyttäisivät laitetasolla tukevan hyvin IPv6-protokollaa. Näin ollen tulosten perusteella voidaan melko luotettavasti olettaa sekä Ciscon että HP:n uusimpien kytkinmallien olevan ominaisuuksiltaan IPv6-protokollaa tukevia ja siten niillä olisi valmius toimia IPv6-osoitteisessa hallintaympäristössä. Toisaalta tutkimustulokset voidaan suoraan liittää ainoastaan tutkittuihin kytkinmalleihin, joten uusien kytkinmallien kohdalla on selvitettävä laitteiden ja ohjelmistojen IPv6-ominaisuuksien toiminnallisuus. Reitittimien kohdalla vastaavia johtopäätöksiä eri valmistajien laitteiden välillä ei voida kattavasti tehdä, koska tutkimuksissa käytetiin ainoastaan kahta eri valmistajan reititintä, joten vertailua muihin reititinmalleihin ei voida tällä otannalla luotettavasti tehdä. Ciscon uusimpien reitittimien kohdalla voitaneen melko turvallisesti todeta IPv6-ominaisuuksien toimivan ongelmitta uusimmilla ohjelmistoversioilla, koska jokainen laboratorioverkossa toimiva Ciscon kytkin saatiin myös toimimaan ongelmitta pelkästään IPv6-protokollan kanssa. Pääsylistatutkimuksilla pyrittiin selvittämään, kuinka IPv6-protokollalla toteutettuja pääsylistoja voidaan konfiguroida kytkimille ja toimivatko pääsylistat samalla tavalla uudemman IP-protokollan kanssa. Tältä osin onnistuttiin hyvin vastaamaan myös pääsylistoja koskeviin tutkimuskysymyksiin ja siten voidaan sanoa myös pääsylistatutkimusten onnistuneen.

Työssä tehdyissä tutkimuksissa otettiin kantaa ainoastaan eri verkkolaitteiden laitekohtaiseen IPv6-protokollatukeen ja siihen, kuinka eri hallinta- ja valvontaprotokollat toimivat yhdessä IPv6-protokollalla toteutetussa ympäristössä. Protokollan käyttöönotto verkkolaitteiden hallinta- ja valvontaosoitteistuksessa vaatii kuitenkin edelleen tutkimustyötä, jotta voidaan varmistua hallinta- ja valvontayhteyksien toimivuudesta IPv6-ympäristössä

myös muilta osin. Tulosten perusteella tutkittava laitekanta voitaisiin ottaa toimivien IPv6-ominaisuuksien takia jatkotutkimuksiin, joissa voitaisiin selvittää laajemmin ja yksityiskohtaisemmin hallinta- ja valvontayhteyksien toiminta muiden järjestelmien ja verkkoteknisten asioiden kanssa. Mahdollisten jatkotutkimusten tavoitteena voisi olla selvittää, kuinka verkkolaitteiden hallinta ja valvonta voitaisiin toteuttaa todellisten etähallinta- ja etävalvontapalvelimien kanssa, kun hallittavat ja valvottavat verkkolaitteet sijaitsevat suurempien verkkokokonaisuuksien takana. Tässä tehdyt tutkimukset eivät esimerkiksi ottaneet kantaa siihen, kuinka verkkojen reititys tulisi toteuttaa tai kuinka IPv6-protokolla voidaan ottaa käyttöön esimerkiksi todellisella etävalvontapalvelimella yhdessä SNMPv3-protkollan kanssa.

LÄHTEET

Barrett, D. & Silverman, R. (2001). SSH, The Secure Shell: the definitive guide. O'Reilly, Sebastopol (CA), 540 p.

Beijnum, I. (2006). Running IPv6. Iljitsch van Beijnum, Berkeley, CA, pp. 16-17.

Brown, S. (2002). Configuring IPv6 For Cisco IOS. International Thomson cop., Syngress Media, London, Rockland, Mass., 362 p.

Case, J., Fedor, M., Schoffstall, M. & Davin, J. (1990). A Simple Network Management Protocol (SNMP), Request for Comments 1157. 36 p. Saatavissa: http://www.ietf.org/rfc/rfc1157.txt?number=1157.

Case, J., Mundy, R., Partain, D. & Stewart, B. (1999). Introduction to Version 3 of the Internet-standard Network Management Framework, Request for Comments 2570. Saatavissa: https://www.ietf.org/rfc/rfc2570.txt.

Cisco. (2009). Cisco IOS IPv6 Configuration Guide - Release 15.0M. Saatavissa (viitattu 22.5.2016): http://www.cisco.com/c/en/us/td/docs/ios/ipv6/configuration/guide/15_0/ipv6_15_0_book.pdf.

Cisco. (2013). Cisco 1800 Series Hardware Installation (Modular) – Overview of Cisco 1800 Series Routers (Modular). Saatavissa (viitattu 9.7.2016): http://www.cisco.com/c/en/us/td/docs/routers/access/1800/1841/hardware/installation/guide/hw/18over.html#wp1053497.

Cisco. (2016a). Catalyst 2960 and 2960-S Software Configuration Guide, 12.2(55)SE - Configuring Interface Characteristics. Saatavissa (viitattu 9.7.2016): http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swint.html#68512.

Cisco. (2016b). Catalyst 2960 and 2960-S Software Configuration Guide, 12.2(55) SE - Configuring IPv6 Host. Saatavissa (viitattu 19.5.2016): http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swipv6.html.

Cisco. (2016c). Catalyst 3750 Software Configuration Guide, Release 12.2(55) SE - Configuring SDM Templates. Saatavissa (viitattu 19.5.2016): http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swsdm.html.

Cisco. (2016d). Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) – Configuring Interface Characteristics. Saatavissa (viitattu 9.7.2016): http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/int_hw_components/configuration_guide/b_int_3se_3850_cg/b_int_3se_3850_cg_chapter_010.html.

Conta, A. & Deering, S. (2006). Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specfication, Request for Comments 4443. 24 p. Saatavissa: https://tools.ietf.org/html/rfc4443.

Cui, Y., Chen, Y., Liu, J., Lee, Y., Wu, J. & Wang, X. (2015). State management in IPv4 to IPv6 transition, IEEE Network, Vol. 29(6), pp. 48-53.

Deering, S. & Hinden, R. (2006). IP Version 6 Addressing Architecture, Request for Comments 4291. 25 p. Saatavissa: https://tools.ietf.org/html/rfc4291.

Deering, S. & Hinden, R. (1998). Internet Protocol, Version 6 (IPv6) Specification, Request for Comments 2460. Saatavissa: https://tools.ietf.org/html/rfc2460.

Desmeules, R. (2003). Cisco Self-Study: Implementing Cisco IPv6 Networks (IPv6) – Configuring IPv6 on Cisco IOS Software Technology. Saatavissa (viitattu 19.5.2016): http://www.ciscopress.com/articles/article.asp?p=31948&seqNum=4.

Goralski, W. (2009). The Illustrated Network: how TCP/IP works in a modern network. Elsevier/Morgan Kaufmann Publishers cop., Amsterdam, Boston, 797 p.

Hinden, R., Deering, S. & Nordmark, E. (2003). IPv6 Global Unicast Address Format, Request for Comments 3587. 5 p. Saatavissa: https://tools.ietf.org/html/rfc3587.

HP. (2016a). HP Switch Software - IPv6 Configuration Guide RA.15.18. 180 p. Saatavissa (viitattu 22.5.2016): http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c04777787.

HP. (2016b). HP Switch Software, IPv6 Configuration Guide WB.15.18. Saatavissa (viitattu 22.5.2016): http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c04777793.

Huitema, C. (2000). Routing in the Internet. 2nd edition, Prentice Hall PTR, Upper Saddle River (NJ), 384 p.

IEEE Standards Association. (1997). Guidelines for 64-bit Global Identifier (EUI-64) General. Saatavissa (viitattu 8.4.2016): https://standards.ieee.org/develop/regauth/tut/eui64.pdf.

Juniper. (2012). Interface Port Naming Conventions SRX Series Services Gateways. Saatavissa (viitattu 9.7.2016): http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/reference/specifications/interfaces-srx-series-port-naming-conventions.html.

Juniper. (2013). Enabling Flow-Based Processing for IPv6 Traffic. Saatavissa (viitattu 21.5.2016): https://www.juniper.net/documentation/en_US/junos12.1x46/topics/task/configuration/interface-security-logical-property-ipv6-traffic-flow-based-processing-enabling-cli.html.

Juniper. (2014). Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery. Saatavissa (viitattu 21.5.2016): http://www.juniper.net/documentation/en_US/junos14.2/topics/topic-map/ipv6-interfaces-neighbor-discovery.html#jd0e127.

Kurose, J. & Ross, K. (2008). Computer Networking: a top-down approach. 4th edition, Pearson, New York, NY, 878 p.

Levin, S. & Schmidt, S. (2014). IPv4 to IPv6: Challenges, solutions, and lessons, Telecommunications Policy, Vol. 38(11), pp. 1059-1068.

Mahmood, H. (2003). Transport Layer Security Protocol in Telnet. APCC 2003 - 9th Asia-Pacific Conference on Communications, in conjunction with 6th Malaysia International Conference on Communications, MICC 2003, Vol. 3, pp. 1033-1037.

McCloghrie, K., Perkins, D. & Schoenwaelder, J. (1999). Structure of Management Information Version 2 (SMIv2), Request for Comments 2578. 43 p. Saatavissa (viitattu 27.12.2015): https://tools.ietf.org/html/rfc2578.

Mun, Y. & Lee, H. (2005). Understanding IPv6. Springer Science+Business Media Inc., Boston, MA, pp. 51-67.

Nadeau, T. (2003). MPLS Network Management: MIBs, tools, and techniques. Morgan Kaufmann cop., San Francisco, California, 592 p.

Narten, T., Nordmark, E. & Simpson, W. (2007). Neighbor Discovery for IP version 6 (IPv6), Request for Comments 4861, 97 p. Saatavissa: https://tools.ietf.org/html/rfc4861.

Narten, T. (1999). Neighbor Discovery and Stateless Autoconfiguration in IPv6. IEEE Internet Computing, Vol. 3(4), pp. 54-62.

Padmavathi, G., Subashini, P. & Aruna, D. (2012). ANODR-ECC Key Management Protocol with TELNET to Secure Application and Network Layer for Mobile Adhoc

Networks, International Journal of Distributed and Parallel Systems (IJDPS), Vol. 3(1), pp. 331-339. Saatavissa (viitattu 29.12.2015): http://airccse.org/journal/ijdps/papers/0112ijdps28.pdf.

Peterson, L. & Davie, B. (2012). Computer Networks: a systems approach. 5th edition, Morgan Kaufmann cop., Burlington (MA), 884 p.

Postel, J. (1981). Internet Protocol, Request for Comments 791. 45 p. Saatavissa: https://tools.ietf.org/html/rfc791.

Postel, J. & Reynolds, J. (1983). Telnet Protocol Specification, Request for Comments 854. 15 p. Saatavissa: http://www.rfc-base.org/txt/rfc-854.txt.

Shaffi, A. & Al-Obaidy, M. (2013). Managing Network Components Using SNMP, International Journal of Scientific Knowledge, Vol. 2(3), pp. 11-18. Saatavissa (viitattu 28.12.2015): http://ijsk.org/uploads/3/1/1/7/3117743/managing_network_components_using_snmp.pdf.

Shin, K., Jung, J., Cheon, J. & Choi, S. (2007). Real-time Network Monitoring Scheme Based On SNMP for Dynamic Information. Journal of Network and Computer Applications, Vol. 30(1), pp. 331-353.

Stallings, W. (2007). Data and Computer Communications. 8th edition, Pearson Prentice Hall, Upper Saddle River (NJ), 878 p.

Stallings, W. (1999). SNMP, SNMPv2, SNMPv3, and RMON 1 and 2. 3rd edition, Addison-Wesley, Reading (MA), 619 p.

Stallings, W. (1998). SNMP and SNMPv2: The infrastructure for network management. IEEE Communications Magazine, Vol. 36(3), pp. 37-43.

Teltumde, P., Meshram, B. & Bansod, T. (2012). Management of Networks Using SNMP, International Journal of Engineering Innovations and Research, Vol. 1(2), pp. 135-138.

Thomson, S., Narten, T. & Jinmei, T. (2007). IPv6 Stateless Address Autoconfiguration, Request for Comments 4862, 30 p. Saatavissa: https://tools.ietf.org/html/rfc4862.

Ylönen, T. & Lonvick, C. (2006). The Secure Shell (SSH) Authentication Protocol, Request for Comments 4252. Cisco Systems Inc., 17 p. Saatavissa: https://tools.ietf.org/html/rfc4252.

Ylönen, T. & Lonvick, C. (2006). The Secure Shell (SSH) Protocol Architecture, Request for Comments 4251. Cisco Systems Inc., 30 p. Saatavissa: https://tools.ietf.org/html/rfc4251.

Ylönen, T. & Lonvick, C. (2006). The Secure Shell (SSH) Transport Layer Protocol, Request For Comments 4253. Cisco Systems Inc. Saatavissa: https://tools.ietf.org/html/rfc4253.

Zheng, F. & Cui, Z. (2010). The New Way of Configuration Management of Network Devices under Mutable Environment, 2010 Third International Symposium on Knowledge Acquisition and Modeling, pp. 103-106.

LIITE A: LABORATORIOVERKON LAITTEIDEN PÄÄSYLISTA-TUTKIMUKSIIN LIITTYVÄT KONFIGURAATIOT

Ciscon kytkimet:

Etäyhteydet estävän pääsylistan konfiguraatiot:

```
ipv6 access-list TESTI
 deny ipv6 2001:2060:BFFD:BFFD::/64 any
 permit ipv6 any any
!
line vty 0 4
 ipv6 access-class TESTI in
!
line vty 5 15
 ipv6 access-class TESTI in
!
```

Etäyhteydet sallivan pääsylistan konfiguraatiot:

```
ipv6 access-list TESTI
 permit ipv6 host 2001:2060:BFFD:BFFD::3 any
 deny ipv6 any any
!
line vty 0 4
 ipv6 access-class TESTI in
!
line vty 5 15
 ipv6 access-class TESTI in
!
```

HP:n kytkimet:

Etäyhteydet estävän pääsylistan konfiguraatiot:

```
ipv6 access-list "TESTI"
     deny ipv6 2001:2060:bffd:bffd::/64 ::/0
     permit ipv6 ::/0 ::/0
     exit
interface x
     ipv6 access-group "TESTI" in
     exit
```

Etäyhteydet sallivan pääsylistan konfiguraatiot:

```
ipv6 access-list "TESTI"
     permit ipv6 2001:2060:bffd:bffd::3/128 ::/0
     deny ipv6 ::/0 ::/0
     exit
interface x
    ipv6 access-group "TESTI" in
    exit
```